Postverlagsort Berlin

MATHEMATISCHE ZEITSCHRIFT

UNTER STÄNDIGER MITWIRKUNG VON

E. KAMKE
TÜBINGEN

R. NEVANLINNA
HELSINKI

F. K. SCHMIDT
HEIDELBERG

HERAUSGEGEBEN VON

H. WIELANDT
TÜBINGEN

WISSENSCHAFTLICHER BEIRAT

W. BLASCHKE A. E. INGHAM H. KNESER
W. MAGNUS O. PERRON G. PICKERT

73. BAND, 1. HEFT

(ABGESCHLOSSEN AM 9. FEBRUAR 1960)

BERLIN · GÖTTINGEN · HEIDELBERG
SPRINGER-VERLAG
1960

Math. Z.

Die **MATHEMATISCHE ZEITSCHRIFT**

wurde im Jahre 1918 von *L. Lichtenstein* unter der Mitwirkung von *K. Knopp*, *E. Schmidt* und *I. Schur* gegründet und herausgegeben. Nach dem Tode Lichtensteins übernahm *K. Knopp* 1933 die Herausgabe. Die Schriftleitung ergänzte sich 1933 durch *E. Kamke* und *F. K. Schmidt*, 1936 durch *R. Nevanlinna* und 1950 durch *H. Wielandt*, der 1952 die Herausgabe übernahm.

---

73. Band **Inhalt** 1. Heft

Seite

NEUMANN, H., and J. WIEGOLD, Linked products and linked embeddings of groups 1

WIELANDT, H., Einbettung zweier Gruppen in eine einfache Gruppe 20

SCHÖNHAGE, A., Über das Wachstum zusammengesetzter Funktionen 22

LILLO, J. C., Continuous Matrices and the Stability Theory of Differential Systems 45

BRUCK, R. H., Some Theorems on Moufang Loops 59

O'KEEFE, E. S., On the independence of primal algebras 79

Unveränderter Nachdruck 1974
Springer-Verlag Berlin Heidelberg New York

NEUMANN, H., and J. WIEGOLD
Math. Zeitschr. 73, 1–19 (1960)

Linked products and linked embeddings of groups

To B. H. NEUMANN on his 50th birthday

By
HANNA NEUMANN and JAMES WIEGOLD

1. Introduction

Recent years have seen the growth of a wide and varied literature concerned with processes of constructing groups as "products" of subgroups in different ways. Amongst the most fruitful concepts in this context is that of a regular product of groups, which was introduced by O. N. GOLOVIN [1] some years ago. The following investigations contribute to the general theme of "products of groups"; the products we consider are not regular, however, although they were suggested by the concept of a regular product.

A group G is said to be a regular product of its subgroups G_α, α ranging over some index set I, if

(i) the groups G_α generate G,

(ii) for each α in I, G possesses a retractive endomorphism π_α mapping the constituent group G_α identically and all the other groups G_β $(\beta \neq \alpha)$ onto the unit element.

This second condition is equivalent to asking that the group G_α intersect the normal closure in G of the subgroup generated by all G_β $(\beta \neq \alpha)$ in the unit element only.

Some time ago, S. MORAN enquired in conversation into the effect of replacing the second condition by the much weaker requirement that each constituent G_α intersect the subgroup generated by the G_β $(\beta \neq \alpha)$ in the unit element only. This remark led us to ask the following question. Given two groups [1]) A and B with normal subgroups X of A and Y of B, does there exist a group G generated by subgroups isomorphic to A and B (denoted by the same letters A and B – a practice we adopt throughout), such that A and B have trivial intersection in G, but the normal closure of A in G meets B exactly in Y, and the normal closure of B in G meets A exactly in X? Loosely speaking this means that mapping A onto the unit element "induces" a homomorphism of G in which B is mapped onto B/Y, and similarly the other way round. Such a group G we call a *linked product of A and B with kernels X and Y*. Clearly, when both X and Y consist of the unit element alone, the linked product becomes a regular product. We exclude this case altogether from our present considerations.

[1]) For convenience, and since we concentrate on this case in the major part of the paper, we describe here the situation for two groups only; some remarks on the general case are found in § 3.

The first question that comes to mind is, of course, whether a linked product of given groups A and B with given kernels X and Y exists. We do not know the answer. The evidence leads us to conjecture that the answer is positive in all cases except one, the certain exception being the case where A and X coincide and have order 2, B also has order 2, and Y is the trivial subgroup (§ 6). On the other hand, it is not difficult to establish the existence of linked products for fairly wide classes of groups. Apart from some special cases obtained by ad hoc methods, we can construct linked products whenever the kernels X and Y are either both non-trivial and finite (using a theorem of H. WIELANDT mentioned below), or whenever one of X and Y is a group which can be generated by any number of pairwise disjoint cycles of not too small orders — to give a rough description at this stage. The methods used are very obviously too awkward to lead any further; at the same time it is precisely these methods that strongly suggest the truth of our conjecture (§§ 5, 6).

By contrast we prove that *linked embeddings* of given groups A and B with given kernels X and Y exist without exception. A linked embedding H differs from a linked product only in that we do not require H to be generated by A and B (§ 4).

In both situations, the linked product and the linked embedding, the case where one kernel — Y say, without loss of generality — is trivial is quite different from that where both kernels are non-trivial. We refer to the two casess as the unsymmetrical and the symmetrical case respectively. The unsymmetrical case seems generally the more difficult one; note that the counterexample mentioned above is of this kind. In both cases reduction theorems play a crucial part. They reduce the case of a linked product or embedding in general to the special case where X coincides with A, and, in the symmetrical case, also Y with B (§ 3). This explains the fact that in our existence theorem only the nature of X and Y matters, while A and B can be arbitrary extensions[2]) of X and Y.

Thus the existence problem in the symmetrical case is reduced to that of finding for given groups X and Y a group Z generated by them in which X and Y intersect trivially, but such that the normal closure of each of X and Y in Z is the whole group Z. This leads immediately to a further interesting problem: Can one find, to given groups X and Y, a simple group Z generated by them so that X and Y have trivial intersection in Z? Clearly not when X and Y are both of order 2. But H. WIELANDT has proved recently [5] that if both X and Y are finite and not both of order 2, then such a simple group Z does in fact exist. Again we conjecture that the restriction to finite groups in unnecessary.

Our tools are once again free products with amalgamations, and wreath products. The former provide the reduction theorems. The wreath product

[2]) We call G an extension of N by M if N is a normal subgroup of G with factor group $G/N \cong M$.

is used to obtain the linked embeddings as well as some cases of unsymmetrical linked products. The more general existence theorems are straightforward applications of a theorem by J. L. BRITTON [2] on the effect of imposing certain relations on a free product of groups.

Properties of generalized free products and of wreath products, as well as a number of other results needed in the course of our investigations, are collected in § 2 for convenient reference.

2. Notation and preliminaries

Groups will always be written multiplicatively, with 1 standing for the unit element (unless otherwise stated) and E the unit subgroup of all groups concerned. We write a^b for $b^{-1}ab$; the commutator $a^{-1}b^{-1}ab$ is abbreviated to $[a, b]$, and analogously the mutual commutator subgroup of two subgroups A and B in a group G is denoted by $[A, B]$; but for the derived group $[G, G]$ we shall usually write G'. The normal closure of a subset M of G, that is the least normal subgroup containing M, is denoted by M^G; if N is a normal subgroup of G, we write $N \lhd G$. If the subset M generates G, we write $G = \mathrm{Gp}(M)$.

The free product of groups G_α, where α runs through an index set I, is denoted by $\prod_{\alpha \in I}^{*} G_\alpha$; the restricted direct product is $\prod_{\alpha \in I}^{\times} G_\alpha$; if I is finite, we may write $G_1 * G_2 * \cdots * G_n$ or $G_1 \times G_2 \times \cdots \times G_n$ instead.

The remainder of this paragraph is devoted to describing the tools and results we need. First two simple well-known facts due to GOLOVIN [1]:

2.1. *If the group G is generated by its subgroups A and B, then $[A, B] \lhd G$, and $A^G = A \cdot [A, B]$.*

2.2. *If A and B are subgroups of G, and φ is any homomorphism of G, then $(A^G)\varphi = (A\varphi)^{G\varphi}$ and $[A, B]\varphi = [A\varphi, B\varphi]$.*

Next some results on generalized free products and group embeddings. Most of these can be conveniently found in B. H. NEUMANN [4], where also the original sources are given.

Let G_α ($\alpha \in I$) be a set of groups containing subgroups $U_{\alpha\beta}$ for each $\beta \neq \alpha$, such that $U_{\alpha\beta} \cong U_{\beta\alpha}$. In certain circumstances there exists a "largest" group G generated by the G_α such that any two constituents G_α and G_β have the prescribed intersection isomorphic to $U_{\alpha\beta}$. This group G is called the generalized free product of the groups G_α with amalgamated $U_{\alpha\beta}$ (again, for a precise definition, cf. [4]). In G_α we form the subgroup U_α generated by all $U_{\alpha\beta}$ ($\alpha \neq \beta$). The following results will be needed:

2.3. [4, 15.6] *The generalized free product of the groups G_α amalgamating $U_{\alpha\beta}$ exists if and only if the generalized free product of the groups U_α amalgamating $U_{\alpha\beta}$ exists.*

2.4. [4, an easy consequence of 15.4] *With the same notation as above, the intersection in G of the subgroup G_α with the subgroup generated by all G_β ($\beta \neq \alpha$) is exactly U_α.*

2.5. [4, 1.1] *With the same notation as above, let φ_α be a homomorphism of G_α into a group Q such that φ_α and φ_β agree where they are both defined, that is on $U_{\alpha\beta}=U_{\beta\alpha}$. Then there is a unique homomorphism φ mapping G into Q such that φ extends every φ_α.*

2.6. [4, 4.1] *Let G be the free product of its subgroups G_α with one amalgamated subgroup U, and let H_α be subgroups of the G_α such that $H_\alpha \cap U = E$ for each α. The subgroup H of G generated by all H_α is the ordinary free product, $H = \prod_\alpha{}^* H_\alpha$, and $H \cap U = E$ in G.*

Next two embedding theorems:

2.7. [4, 17.1 and 18.3] *If G is an arbitrary group containing a pair of isomorphic subgroups A and B, then there exists a group H containing G such that A and B are conjugate under H. If G is finite, H can be chosen finite.*

2.8. [3, 4.2] *Every group G can be embedded in the derived group H' of some group H. If G is finite, H can be chosen finite.*

In fact rather more can be said about the structure of the group H in this last result, but we shall not need this. The result is obtained using wreath products, which are described in full in that context. As we shall need two further simple properties of wreath products not mentioned in [3], we shall repeat their definition here before stating these properties.

To form the (unrestricted) wreath product $A \operatorname{Wr} B$ of two non-trivial groups A and B, we consider first the group of all functions $f(b)$, $b \in B$, defined on B and taking values in A, with multiplication given by

$$(fg)(b) = f(b) \cdot g(b) \quad \text{for all } b \in B.$$

This is, of course, the unrestricted direct product of as many copies of A as the order of B indicates. In particular, all those functions whose value is the unit element of A for all except one fixed argument b form a group isomorphic to A, which we denote by A_b. Its elements are often conveniently denoted by a_b indicating the particular function which at the argument b takes the value $a \in A$. Now we extend this group of functions by a group isomorphic to B (again denoted by B) to obtain $A \operatorname{Wr} B$: $A \operatorname{Wr} B$ is the group generated by all functions f and all elements b_1 in B with the relations:

$$b_1^{-1} f b_1 = f_1, \quad \text{where} \quad f_1(b) = f(b b_1^{-1}) \quad \text{for all } b \in B.$$

To obtain the restricted wreath product $A \operatorname{wr} B$, we use the restricted direct product instead of the unrestricted one, that is we consider only those functions f which take the value 1 in A for all but a finite number of arguments.

In this context we find it convenient to denote the isomorphic copy A_b of A corresponding to the unit element of B by A_e rather than by A_1.

LEMMA 2.9. *In the restricted wreath product $G = A \operatorname{wr} B$,*

$$A_e \cap B^G = A_e'.$$

PROOF. Firstly B^G contains $[A_b, B]$ for any fixed $b \in B$. Hence for any $a \in A$, and any $b \neq 1$ in B, B^G contains the commutator $a_b^{-1} b a_b b^{-1} = a_b^{-1} a_e$.

Next let c be any further element of A; as B^G is normal in G, it contains the element

$$(a_b^{-1}a_c)^{-1}(a_b^{-1}a_c)^{c_c} = a_c^{-1}a_b a_b^{-1}a_c^{c_c} = [a_c, c_c].$$

Hence B^G contains all commutators, that is all generators of A_c'; thus B^G, and therefore $A_c \cap B^G$, contains A_c'.

To prove the inclusion the other way round, we observe first of all that $A_c^G = A_c \cdot [A_c, B]$ and $B^G = B \cdot [A_c, B]$ by 2.1. Let then x be any element of $A_c \cap B^G$; as an element of B^G it has an expression

$$x = b\,u$$

with $b \in B$, $u \in [A_c, B]$. But this means that

$$b = x\,u^{-1} \in B \cap A_c[A_c, B] = B \cap A_c^G = E;$$

we conclude that $b = 1$, and hence that $x = u \in [A_c, B]$.

Next, $[A_c, B]$ is generated by all commutators of the form $[a_c, b] = a_c^{-1}a_b$; since the inverse of such an element has the same form we see that

$$x = a_{1c}^{-1}a_{2c}^{-1}\dots a_{rc}^{-1}a_{1b_1}a_{2b_2}\dots a_{rb_r},$$

for some $r \geqq 1$, where we may assume that each $b_i \neq 1$. As $x \in A_c$ this means that

(i) $$a_{1b_1}a_{2b_2}\dots a_{rb_r} = 1,$$

(ii) $$a_{1c}^{-1}a_{2c}^{-1}\dots a_{rc}^{-1} = x.$$

The next step of the proof is to collect together all the terms from the same component in the left hand side of (i) and apply the same permutation to the left hand side of x^{-1} as given by (ii). Equation (i) now becomes

(iii) $$a_{b_1}'a_{b_2}''\dots a_{b_s}^{(s)} = 1;$$

where we have renamed where necessary, and where moreover $b_i \neq b_j$ if $i \neq j$. The result on x^{-1} of the corresponding operation is:

(iv) $$a_c'a_c''\dots a_c^{(s)} \equiv x^{-1} \pmod{A_c'}.$$

Now (iii) implies that $a_{b_1}' = a_{b_2}'' = \dots a_{b_s}^{(s)} = 1$; because of the isomorphism between A_c and the components A_{b_i}, we therefore also have that $a_c' = a_c'' = \dots a_c^{(s)} = 1$. The congruence (iv) therefore tells us that $x \in A_c'$, and this completes the proof of the lemma.

We omit the proof of the following very simple lemma:

LEMMA 2.10. (i) *If A is an abelian group, and B a group containing an element b of finite order n, then the subset $\hat{A}$ of A wr B consisting of all elements of the form*

$$a_c^{-1}a_b 1_{b^2}\dots 1_{b^{n-1}}$$

is a subgroup isomorphic with A.

(ii) *If A is an abelian group, and B any group containing an element b of infinite order, then the subset $\hat{A}$ of $A \operatorname{Wr} B$ consisting of the functions f_a for which*

$$f_a(b^n) = a^{(-1)^{n+1}},$$
$$f_a(x) = 1 \text{ if } x \notin \operatorname{Gp}(b),$$

is a subgroup isomorphic with A.

Note that both lemma 2.10 (i) and the first inclusion proved in lemma 2.9 hold equally well in the unrestricted wreath product; but we shall need the facts only as stated.

Finally we come to a description of the theorem by J. L. BRITTON [2] on free products of groups. Let P be the free product of its non-trivial subgroups G_α ($\alpha \in I$). Every element $g \in P$ has a unique representation of the form $g = y_1 y_2 \dots y_n$, $y_i \neq 1$, $y_i \in G_{\alpha_i}$ with $\alpha_i \neq \alpha_{i+1}$. We call n the *length* of g, $n = l(g)$. If y_1 and y_n belong to different constituent groups, we call g *cyclically reduced*. In that case all the cyclic rearrangements of g, that is the n elements

$$y_\lambda y_{\lambda+1} \dots y_n y_1 \dots y_{\lambda-1} \qquad (\lambda = 1, 2, \dots, n)$$

are also cyclically reduced and of length n.

If g and h are arbitrary elements of P, define $\beta(g, h)$ and $\varepsilon(g, h)$ as the number of cancellations and amalgamations necessary to bring the product gh into normal form, and let $\alpha(g, h) = \beta(g, h) + \varepsilon(g, h)$. Obviously $\varepsilon(g, h)$ is 0 or 1, and

$$l(gh) = l(g) + l(h) - 2\beta(g, h) - \varepsilon(g, h).$$

Now let Ω be a subset of P such that all elements of Ω are cyclically reduced and of length at least 2. BRITTON's theorem gives information on the effect of imposing the relations $\omega = 1$ ($\omega \in \Omega$) on P, under certain conditions now to be formulated:

Let Ω^* be the set consisting of all the cyclic rearrangements of elements of Ω, and their inverses, and assume that Ω has the following property[3]):

2.11. *If $u, v \in \Omega^*$ and $uv \neq 1$, then $6\alpha(u, v) < \operatorname{Min}(l(u), l(v))$.*

Then the relevant part of BRITTON's theorem states:

2.12. *Every element in the normal closure Ω^P of Ω in P has length at least equal to* $\operatorname{Min}_{\omega \in \Omega} l(\omega)$.

In our applications P will be a free product of two groups and Ω will usually consist of a single element, so that checking the conditions 2.11 is a matter of easy, though laborious routine. In our case the shortest length of any element in Ω will always be at least 3. BRITTON's result then ensures, of course, that in the factor group P/Ω^P the constituent groups are isomorphically represented and the trivial intersection is preserved.

[3]) At the Eleventh British Mathematical Colloquium in September 1959 J. L. BRITTON announced that the constant 6 in 2.11 can now be replaced by 5 — which is best possible.

3. Linked products and embeddings; reduction theorems

We start with the formal definitions of linked products and linked embeddings of two groups, and discuss the different definitions arising when more than two groups are involved.

Let A and B be groups possessing normal subgroups X and Y respectively.

Definition 3.1. *The group G is called a linked product of its subgroups A and B with kernels X and Y if*

(i) *G is generated by A and B,*

(ii) *$A \cap B = E$ in G,*

(iii) *$A^G \cap B = Y$ and $B^G \cap A = X$.*

Definition 3.2. *The group G is called a linked embedding of its subgroups A and B with kernels X and Y if conditions* (ii) *and* (iii) *of* 3.1 *hold.*

When one considers linked products or embeddings of more than two factors A_α (α in some index set I) with kernels X_α, several possibilities arise. Condition (ii) can become one of the following three conditions:

3.3 (ii) a) For any division of the index set I into two non-empty disjoint subsets I' and I'',

$$\operatorname*{Gp}_{\alpha \in I'}(A_\alpha) \cap \operatorname*{Gp}_{\beta \in I''}(A_\beta) = E \quad \text{in } G.$$

b) If $A^\alpha = \operatorname*{Gp}_{\beta \neq \alpha}(A_\beta)$, then $A^\alpha \cap A_\alpha = E$ in G for each $\alpha \in I$.

c) $A_\alpha \cap A_\beta = E$ in G for each pair $\alpha \neq \beta$ in I.

Clearly a) implies b) and b) implies c).

Similarly, condition (iii) can become one of the following:

3.3 (iii) a) For any division of the index set I into two non-empty disjoint subsets I' and I'',

$$\left(\operatorname*{Gp}_{\alpha \in I'}(A_\alpha)\right)^G \cap A_\beta = X_\beta \quad \text{for each } \beta \in I''.$$

b) $(A^\beta)^G \cap A_\beta = X_\beta$ for each $\beta \in I$.

c) $A_\alpha^G \cap A_\beta = X_\beta$ for each $\beta \neq \alpha$ in I.

Here again a) implies b) and c); but neither of b) and c) implies the other. We give two examples to show this — the second will also be used (§ 6) in a different context.

Example 3.4. Let G be a linked product of four groups A_α each coinciding with its kernel X_α, which is an infinite cycle generated by x_α ($\alpha = 1, 2, 3, 4$). Specifically, G is generated by the x_α with the defining relations

$$x_1 x_2 x_1 = x_2 x_1 x_2, \qquad x_3 x_4 x_3 = x_4 x_3 x_4,$$
$$[x_1, x_3] = [x_1, x_4] = [x_2, x_3] = [x_2, x_4] = 1.$$

Then $G = G_1 \times G_2$, where $G_1 = \operatorname{Gp}(x_1, x_2)$ and $G_2 = \operatorname{Gp}(x_3, x_4)$ are two isomorphic copies of Artin's braid group on two generators; these are locally infinite and the two generators have no power other than the unit element in common.

Therefore the constituents X_α of G satisfy the strongest intersection property (ii) a). The group G also satisfies (iii) b) since mapping any three of the generators onto the unit element reduces the remaining one to the unit element as well. But (iii) c) is not satisfied in G, because mapping x_1 onto 1 results in x_2 becoming 1, but x_3 and x_4 are not affected, that is

$$X_1^G \cap X_2 = X_2, \quad \text{but} \quad X_1^G \cap X_3 = X_1^G \cap X_4 = E.$$

EXAMPLE 3.5. Let G be the dihedral group of order 8 generated by elements a, b subject to the relations $a^4 = b^2 = (ab)^2 = 1$. As the constituents of our linked product we take the subgroups

$$A_1 = \mathrm{Gp}(a), \quad A_2 = \mathrm{Gp}(b), \quad A_3 = \mathrm{Gp}(ab) \text{ with } X_1 = \mathrm{Gp}(a^2), \quad X_2 = X_3 = E.$$

A_1, A_2 and A_3 obviously together generate G, and satisfy intersection properties (ii) c). On the other hand, it is easy to verify the following equalities:

$$A_2^G \cap A_1 = A_3^G \cap A_1 = \mathrm{Gp}(a^2),$$
$$A_1^G \cap A_2 = A_3^G \cap A_2 = E,$$
$$A_1^G \cap A_3 = A_2^G \cap A_3 = E.$$

Thus the normal closure conditions (iii) c) are satisfied: however, (iii) b) is definitely not satisfied, since $A^1 = A^2 = A^3 = G$.

In all cases of linked products and embeddings we have to distinguish between the case where all the kernels X_α are non-trivial — in that case the product or embedding is called *symmetrical* — and the case where some, but not all, of the kernels are the unit group, when the product or embedding is called ***unsymmetrical***. In almost all contexts, these two cases require different treatment.

We are now ready to prove the theorems which reduce the question whether a linked product of given groups A_α with given kernels X_α exists to the special case where A_α and X_α coincide for all those constituents where X_α is non-trivial. We give the full proofs in the case of two factors only: the proof of the corresponding theorems for any of the possible linked products or embeddings of more than two groups requires only minor modifications, which are easily pointed out at the end.

THEOREM 3.6 (The symmetrical case). *Let Z be a linked product (embedding) of two non-trivial groups X and Y with kernels X and Y. If A is an arbitrary extension of X and B an arbitrary extension of Y, there exists a linked product (embedding) of A and B with kernels X and Y.*

Proof. We construct a linked product (embedding) explicitly. It is convenient to begin by listing the properties of Z:

(i) $Z = \mathrm{Gp}(X, Y)$,

(ii) $X \cap Y = E$ in Z,

(iii) $X^Z \geqq Y$ and $Y^Z \geqq X$.

If Z is merely a linked embedding, (i) has to be replaced by the inclusions $X \subseteqq Z$, $Y \subseteqq Z$. If Z is a linked product, note that $X^Z = Y^Z = Z$ (and the corresponding fact is true also in each of the three possible cases of products of more than two factors: the normal closures appearing in the conditions become the whole of the linked product as soon as $A_\alpha = X_\alpha$ for each α).

Now let G be the generalized free product of A, B and Z amalgamating E between A and B, X between A and Z, and Y between B and Z. That this exists follows from 2.3: the amalgamations generate X in A, Y in B, and Z in Z. But the generalized free product of X, Y and Z amalgamating E between X and Y, X between X and Z, and Y between Y and Z, is obviously Z itself. In order to prove that G is a linked product (embedding) of A and B with kernels X and Y, we have to prove:

(iv) $G = \mathrm{Gp}(A, B)$ (or, for embedding, the trivial fact that A and B are contained in G),

(v) $A \cap B = E$ in G,

(vi) $A^G \cap B = Y$, $B^G \cap A = X$.

To prove (iv), note that G is generated by A, B and Z. But Z is generated by X and Y, and the facts that $X \subseteqq A$ and $Y \subseteqq B$ now prove (iv).

(v) is immediate from the definition of G.

To prove (vi), it is sufficient to prove just one of the two statements. Now by (iii),

$$A^G \supseteqq A^Z \supseteqq X^Z \supseteqq Y,$$

so that

$$A^G \cap B \supseteqq Y.$$

For the proof that the normal closure of A in G, that is, the smallest normal subgroup of G containing A, does not intersect B in more than Y, it is sufficient to exhibit just one normal subgroup N of G which is such that $N \supseteqq A$ and $N \cap B = Y$. Because then $N \supseteqq A^G$, which of course implies that

$$Y = N \cap B \supseteqq A^G \cap B.$$

To find such an N, we use 2.5: consider the group $Q = B/Y$, and the homomorphisms

$$\varphi_1 \colon A \to E \subseteqq Q,$$
$$\varphi_2 \colon B \to B/Y = Q \quad \text{canonically},$$
$$\varphi_3 \colon Z \to E \subseteqq Q.$$

These homomorphisms clearly agree on the amalgamations of A, B and Z in G. There exists, therefore, a homomorphism φ mapping G onto B/Y in such a way that φ agrees with φ_1, φ_2, φ_3 on the constituents A, B and Z. Since in particular $B\varphi = B/Y$, it follows that the kernel N of φ intersects B in Y; and as $A\varphi = E$, N contains A.

This completes the proof of the reduction theorem. We add some remarks:

REMARK 1. If in the last part of the proof, we take Q instead as the direct product $A/X \times B/Y$ and consider the canonic homomorphism φ_1: $A \to A/X \leqq Q$, in place of the φ_1 chosen above, the result obtained is: $X^G \cap B = Y$ in G, and similarly one shows also that $Y^G \cap A = X$. In other words, the particular linked product (embedding) G we have constructed above is such that if

$$X_1 \lhd A, \quad X \leqq X_1 \leqq A, \quad \text{and} \quad Y_1 \lhd B, \quad Y \leqq Y_1 \leqq B,$$

then $X_1^G \cap B = Y$ and $Y_1^G \cap A = X$. This property will of course not be satisfied in general.

REMARK 2. If more than two groups are involved, the assumptions of the theorem will be the existence of a linked product or embedding Z of the groups X_α, that is of a group Z satisfying one of the intersection properties and one of the normal closure properties obtained by identifying in one of 3.3 (ii) a), b) or c) and in one of 3.3 (iii) a), b) or c) the group A_α with X_α for each α. The linked product or embedding G of the extensions A_α of the X_α will now again be constructed as the generalized free product of the group Z and all the A_α, amalgamating X_α between Z and A_α, and E between A_α and A_β, $\alpha \neq \beta$. That G then satisfies the corresponding intersection and normal closure properties is again a consequence of the special properties of a generalized free product; in particular, the property 2.4 will provide the intersection property in G (which is no longer as trivial as in the case of two factors above).

THEOREM 3.7 (The unsymmetrical case). *Let U be a linked product (embedding) of its non-trivial subgroups X and B with kernels X and E. If A is any extension of X, there exists a linked product (embedding) of A and B with kernels X and E.*

Proof. Again we begin by listing the properties of U:

(i) $U = \mathrm{Gp}(X, B)$ — or $X \leqq U$, $B \leqq U$,

(ii) $X \cap B = E$ in U,

(iii) $X^U \cap B = E$ and $B^U \geqq X$.

We form the free product G of U and A amalgamating X. We have then to prove:

(iv) $G = \mathrm{Gp}(A, B)$ — or $A \leqq G$, $B \leqq G$,

(v) $A \cap B = E$ in G,

(vi) $A^G \cap B = E$ and $B^G \cap A = X$.

The first of these is immediate, since in the case of a linked product, U is generated by X and B, and of course $X \leqq A$.

We prove (vi) next, as (v) is then an obvious corollary. To prove the first part, it suffices to exhibit a normal subgroup N of G containing A and meeting B in E. Again we use 2.5: by (iii) there exists a homomorphism φ_1 of U mapping X onto E and mapping B identically. It agrees on the amalgamated subgroup X with the homomorphism φ_2 mapping A onto E. There

exists therefore a homomorphism φ of G continuing both φ_1 and φ_2. The kernel N of φ contains A and intersects B trivially.

For the second part of (vi), we first note that

$$B^G \cap A \geqq B^U \cap A \geqq X \cap A = X;$$

to show that the intersection is not greater than X, we need to find a normal subgroup of G which contains B and intersects A in X. Now the mappings

$$\psi_1\colon\ U \to E$$

$$\psi_2\colon\ A \to A/X \quad \text{canonically}$$

agree on the amalgamated subgroup X. Therefore there exists a homomorphism ψ of G continuing both ψ_1 and ψ_2. Its kernel is readily seen to be a normal subgroup of the desired kind. This completes the proof of theorem 3.8.

Again the treatment for several factors is analogous: U will be given as linked product of the non-trivial kernels X_α and those constituents A_β whose kernels are trivial, satisfying one of the intersection and one of the normal closure properties 3.3. For arbitrary extensions A_α of the X_α, G will be constructed as the generalized free product of U and the A_α, amalgamating X_α between U and A_α, and E between any of the groups A_α. The properties 2.4 and 2.5 of the generalized free product will then ensure that the correct intersection and normal closure properties which are given in U are also satisfied in G by all the constituents A_α and A_β.

We note particularly that the reduction theorems 3.6 and 3.7 give sufficient conditions for the existence of a linked product of A and B with kernels X and Y. That the existence of the "reduced" linked product is definitely not necessary is shown by the examples in § 6.

Two further remarks, though different in nature from the reduction theorems proper, nevertheless belong to this section, as they provide for the construction of new linked products from other simpler ones.

THEOREM 3.8. *Let G_α be a linked product of X_α and Y with kernels* (i) *X_α and Y, or* (ii) *X_α and E, or* (iii) *E and Y, for each α in some index set I; then the free product G of the groups G_α with the one amalgamated subgroup Y is a linked product of the ordinary free product $X = \prod_{\alpha \in I}^{*} X_\alpha$ and Y with kernels* (i) *X and Y, or* (ii) *X and E, or* (iii) *E and Y respectively.*

Proof. By 2.6 the subgroups X_α generate in G their free product X, and its intersection with the amalgamated subgroup Y is E. Also, as each G_α is generated by X_α and Y, G is generated by X and Y.

Next, if $X_\alpha^{G_\alpha} \geqq Y$ for all α, then a fortiori $X^G \geqq Y$. And also, if $Y^{G_\alpha} \geqq X_\alpha$ for each α, then $Y^G \geqq X$. It remains to prove:

for (ii): if $X_\alpha^{G_\alpha} \cap Y = E$ then $X^G \cap Y = E$, and

for (iii): if $Y^{G_\alpha} \cap X_\alpha = E$ then $Y^G \cap X = E$.

The first assumption implies that there exist homomorphisms φ_α mapping G_α onto Y, namely those mapping X_α onto E and mapping Y identically.

This means that the φ_α agree on the amalgamated subgroup Y, and by 2.5 there exists a homomorphism φ mapping G onto Y which continues the φ_α. Its kernel is a normal subgroup containing all the X_α, and therefore X, but meeting Y in the trivial group. Therefore, a fortiori, $X^G \cap Y = E$.

The proof of the second statement is analogous and we omit it.

THEOREM 3.9. *Let G_α be a linked product of X_α and Y_α with kernels* (i) *X_α and Y_α, or* (ii) *X_α and E, for each α in some index set I. Then the direct product $G = \prod_{\alpha \in I}^{\times} G_\alpha$ is a linked product of $X = \prod_{\alpha \in I}^{\times} X_\alpha$ and $Y = \prod_{\alpha \in I}^{\times} Y_\alpha$ with kernels* (i) *X and Y, or* (ii) *X and E respectively.*

The proof is immediate using standard properties of the direct product, in particular the following: if $G = \prod^{\times} G_\alpha$ and X_α is a subgroup of G_α for each α, then

$$\prod^{\times} X_\alpha^{G_\alpha} = (\prod^{\times} X_\alpha)^G = X^G.$$

4. Linked embeddings

From this point onwards we shall restrict our attention to linked products and embeddings of just two groups. In this short section we are going to establish the existence of linked embeddings, both symmetrical and unsymmetrical, without exception.

THEOREM 4.1. *For any two groups A and B with normal subgroups X and Y respectively, there exists a linked embedding of A and B with kernels X and Y.*

For the proof, we bear in mind the simplification of the problem due to the reduction theorems of the last section. Assuming, as before, X to be certainly non-trivial, we may now further assume that A coincides with X. The proof of theorem 4.1 is split into two parts:

1. Proof of the unsymmetrical case. We are given two non-trivial groups X and B and wish to find a group H containing them both, in such a way that in H the normal closure of X meets B trivially, but the normal closure of B contains X. Let X be embedded into the derived group of some group X_1 (cf. 2.8), and form the restricted wreath product $H = X_1 \operatorname{wr} B$ of X_1 by B. By lemma 2.9, $B^H \geqq X_1' \geqq X$ (we have here identified X_1 with $(X_1)_e$), and of course $X_1^H \cap B = E$ so that also $X^H \cap B = E$. Hence H is a linked embedding of X and B with kernels X and E, as required.

Again, by 2.8, X_1 can be taken finite when X is finite. Therefore:

COROLLARY 4.2. *To any two finite groups X and B there exists a finite linked embedding of X and B with kernels X and E.*

If X coincides with its derived group, the first step in our construction is superfluous, and $H = X \operatorname{wr} B$ is a linked product of X and B with kernels X and E.

COROLLARY 4.3. *If X is a perfect group, there exists a linked product of X and B with kernels X and E, for arbitrary B. If both X and B are finite, the linked product can be taken finite.*

2. Proof of the symmetrical case. This time we are given non-trivial groups X and Y which we wish to embed so that they intersect trivially, but the normal closure of each contains the other. We take an isomorphic copy $\overline{X}$ of X and form a group H_1 as in the unsymmetrical case, such that $Y^{H_1} \geqq \overline{X}$. Next we repeat the same procedure: embed H_1 in the derived group of some group H_2, and form the wreath product $H_3 = H_2 \operatorname{wr} X$. H_3 now contains the isomorphic groups X and $\overline{X}$; by 2.7 we can embed H_3 in a group H such that X and $\overline{X}$ are conjugate under H. We claim that H is a linked embedding of X and Y with kernels X and Y.

Firstly $X \cap Y = E$, because $H_2 \cap X = E$ and $Y \subseteq H_2$.

Next we examine the normal closures of X and Y in H: it follows from 2.9 (identifying H_2 with $(H_2)_e$ in $H_2 \operatorname{wr} X$) that

$$X^H \geqq X^{H_2} \geqq H_2', \quad \text{and} \quad H_2' \geqq H_1 \geqq Y.$$

Also $Y^H \geqq Y^{H_1} \geqq \overline{X}$; but Y^H is normal in H, and X and $\overline{X}$ are conjugate in H, so that $Y^H \geqq X$ as required.

Again, if X and Y are finite, every step can be done using finite groups (2.7 and 2.8). Hence:

COROLLARY 4.4. *To any two finite groups X and Y there exists a finite linked embedding of X and Y with kernels X and Y.*

Our procedure in the symmetrical case is really unnecessarily complicated. One may instead take an arbitrary regular product of X and Y – for example $X \times Y$, which is finite when X and Y are – and embed this in a simple group. This argument also allows one to deduce Corollary 4.4. Our proof above was used as a straightforward continuation of the proof in the unsymmetrical case, which, moreover, avoided the theorem that any group can be embedded in a simple group. Though this is well-known (as a consequence of 2.7, or using possibly infinite permutation groups), we know of no explicit proof in the literature to which we could refer.

In spite of corollaries 4.2, 4.3 and 4.4, our linked embeddings of two arbitrary groups A and B are invariably infinite when A and X do not coincide – this is because the generalized free products used in theorems 3.6 and 3.7 will be infinite in these cases. Nevertheless we believe that any two finite groups A and B possess a finite linked embedding, even though our methods do not establish this.

5. Linked products: the symmetrical case

As mentioned in the introduction, H. WIELANDT has proved [5] that to any two finite non-trivial groups X and Y not both of which have order 2, there exists a finite simple group Z generated by X and Y, in which X and Y have only the unit element in common. Clearly, Z is a linked product of X and Y with kernels X and Y.

If both X and Y are of order 2, the symmetric group of degree three is clearly a linked product of X and Y with kernels X and Y, because it is generated by two transpositions, and the normal closure of each is the whole group. We have therefore:

THEOREM 5.1. *If X and Y are arbitrary finite groups, there exists a finite linked product of X and Y with kernels X and Y.*

The reduction theorem 3.6 now gives:

COROLLARY 5.2. *If A and B are arbitrary groups with finite normal subgroups X and Y respectively, there exists a linked product of A and B with kernels X and Y.*

For the rest we have recourse to BRITTON's theorem, motivated by the following observation:

LEMMA 5.3. *Let G be a linked product of its subgroups X and Y with kernels X and Y. Then $G' = [X, Y]$ and*

$$G/G' \cong X/X \cap G' \cong Y/Y \cap G'.$$

Proof. As $X^G \geqq Y$ and $Y^G \geqq X$, we have

$$X^G = Y^G = G.$$

Using 2.1, that is $[X, Y] \lhd G$ and $X^G = X \cdot [X, Y]$ and $Y^G = Y \cdot [X, Y]$, it follows that for the canonic homomorphism φ of G onto $G/[X, Y]$,

$$X\varphi = Y\varphi = G\varphi,$$

and therefore by 2.2:

$$[G, G]\varphi = [G\varphi, G\varphi] = [X\varphi, Y\varphi] = [X, Y]\varphi = E.$$

This means that $G' \leqq [X, Y]$, hence that $G' = [X, Y]$. Finally, the equality $G = XG' = YG'$ gives

$$G/G' \cong X/X \cap G' \cong Y/Y \cap G'.$$

COROLLARY 5.4. *If X and Y are finite, of coprime orders, then any linked product of X and Y with kernels X and Y coincides with its derived group.*

Because G/G' is isomorphic to a factor group both of X and of Y.

From lemma 5.3 it is clear that if it is possible to impose on the free product $X * Y$ relations identifying X and Y modulo the subgroup $[X, Y]$, the result will be a linked product of X and Y with kernels X and Y, provided the relations do not damage the constituents X and Y or their trivial intersection.

We begin with the case of two cycles.

LEMMA 5.5. *Let X and Y by cyclic groups generated ba x and y respectively, and let P be their free product. Let further ω be the element*

$$\omega = x y^{-1} \prod_{k=2}^{l} [x^k, y]$$

of P, where, denoting the order of y by $|y|$,

$$(1)\quad l=6 \quad \textit{when } |y|>2,$$

$$(2)\quad l=10 \quad \textit{when } |y|=2.$$

Then the set Ω consisting of the single element ω satisfies the assumption 2.11 *of Britton's theorem* 2.12, *provided that in the case* (1), $|x|>12$, *and in the case* (2), $|x|>20$.

The proof consists in a straightforward check: ω is cyclically reduced, of length 22 when $l=6$, and of length 38 when $l=10$. One has to confirm that the number of cancellations and amalgamations between ω and its cyclic rearrangements and their inverses is at most 3 in the first case, and at most 6 in the second[4]).

LEMMA 5.6. *Let X be an infinite cycle generated by x, and Y an arbitrary group generated by elements y_α, finite or infinite in number, such that $y_\alpha \neq y_\beta^{\pm 1}$ if $\alpha \neq \beta$. For each α consider the element*

$$\omega_\alpha = x\, y_\alpha^{-1} \prod_{k=2}^{l_\alpha} [x^k, y_\alpha],$$

where $l_\alpha=10$ when $|y_\alpha|=2$, $l_\alpha=6$ when $|y_\alpha|>2$. Then the set Ω consisting of all the elements ω_α satisfies the assumption 2.11 *of Britton's theorem* 2.12.

Proof. Again one has to check that, when multiplied together, any two elements of the set Ω^* (obtained by adding all cyclic rearrangements of the ω_α and their inverses to Ω) cancel and amalgamate less than one sixth of the length of the smaller one. If $u, v \in \Omega^*$, and u, v are cyclic rearrangements of the same element ω_α, this follows at once from lemma 5.5. If they are cyclic rearrangements (or inverses of such) of two distinct elements ω_α and ω_β, the number $\alpha(u, v)$ of cancellations and amalgamations is at most 2, since only a power of x can cancel; the neighbouring factors $y_\alpha^{\varepsilon_\alpha}$ and $y_\beta^{\varepsilon_\beta}$ can only amalgamate.

THEOREM 5.7. *If X is an infinite cycle and Y an arbitrary group, then there exists a linked product Z of X and Y with kernels X and Y.*

Proof. Let Y be generated by elements y_α, in such a way that $y_\alpha \neq y_\beta^{\pm 1}$ if $\alpha \neq \beta$, and consider the set Ω of elements ω_α as given in lemma 5.6. Then, with $P = X * Y$, it follows from BRITTON's theorem 2.12 that the group $Z = P/\Omega^P$ is generated by X and Y, and that $X \cap Y = E$ in Z.

Also, the relation $\omega_\alpha = 1$ holds in Z for each α, so that in particular

$$x^{-1} = y_1^{-1} \prod_{k=2}^{l_1} [x^k, y_1],$$

[4]) The information given in footnote 3) has not been used here. It would result in slightly smaller bounds for l, and therefore slightly better bounds for the order of x.

and as X is generated by x, this proves that $X \leqq Y \cdot [X, Y] = Y^Z$. Similarly we can rewrite the relation $\omega_\alpha = 1$ to read

$$y_\alpha = \left(\prod_{k=2}^{l_\alpha} [x^k, y_\alpha] \right) x \quad \text{for all } \alpha,$$

and as the y_α generate Y, this means that

$$Y \leqq [X, Y] \cdot X = X^Z,$$

as required.

The method of using lemmas 5.5 and 5.6 can clearly be extended a little further. In the first place let X be generated by elements x_α, finite or infinite in number, where we assume that $x_\alpha^m \neq x_\beta^n$ unless $x_\alpha^m = x_\beta^n = 1$, and take Y as a cyclic group generated by y. The set Ω consisting of words

$$\omega_\alpha = x_\alpha y^{-1} \prod_{k=2}^{l_\alpha} [x_\alpha^k, y]$$

will again satisfy the condition 2.11, provided the numbers l_α, $|x_\alpha|$, $|y_\alpha|$ are subject to the same restrictions as l, $|x|$ and $|y|$ in lemma 5.5. The argument is just as before: cyclic transforms of different elements ω_α and ω_β cannot cancel too much of each other because of the restriction $x_\alpha^m \neq x_\beta^n$. Then again, one can extend this to cover an arbitrary group Y generated by elements y_α with the only (trivial) assumption $y_\alpha \neq y_\beta^{\pm 1}$, by introducing sufficiently many relations of the form

$$y_\beta x_\alpha^{-1} = \Pi [x_\alpha^k, y_\beta]$$

to ensure that $X \leqq Y \cdot [X, Y]$ and $Y \leqq X \cdot [X, Y]$.

This will establish the existence of a linked product of a group X which can be generated by non-intersecting cycles of suitably restricted orders, and an arbitrary group Y, with kernels X and Y.

We refrain from going into further details: in specific cases suitable relations can usually be constructed, and the verifications are mostly not too difficult. But to find relations which will serve uniformly, that is, which will enable us to prove the existence of a linked product for all groups X and Y by this method, is hardly feasible.

6. Linked products: the unsymmetrical case

We begin with a lemma which leads the way to the counterexample announced in the introduction.

LEMMA 6.1. *Let G be a linked product of its subgroups X and B with kernels X and E. Then $X \leqq [B, X]$.*

Proof. By definition G is generated by X and B in such a way that $B^G \geqq X$ and $X^G \cap B = E$. Now $B^G = B \cdot [B, X]$ and $X^G = X \cdot [B, X]$, so that an arbitrary element $x \in X$ has a representation

$$x = bu,$$

with $b \in B$, $u \in [B, X]$. Hence $b = xu^{-1} \in X^G$, and therefore $b \in X^G \cap B$. Thus $b = 1$, and $x = u \in [B, X]$. As x was arbitrary, it follows that $X \subseteq [B, X]$, as required.

EXAMPLE 6.2. *Let X and B be of order 2. Then there is no linked product of X and B with kernels X and E.*

Proof. If there were a linked product G, then by lemma 6.1 we must have $X \subseteq [B, X]$.

Now X is generated by x, B is generated by b, where $x^2 = b^2 = 1$. Therefore $[B, X]$ has the single generator $[b, x]$, so that

$$x = [b, x]^k$$

for some positive integer k. However, as b and x both have order 2, this equation reduces to

$$1 = x^{b(bx)^{k-1}},$$

giving $x = 1$, in contradiction to the assumptions.

Nevertheless, linked products with kernels X and E, where the order of X is 2, may exist even when B is again of order 2, showing that the reduction theorem 3.7 provides in fact only a sufficient condition. For an example, we again use the dihedral group of order 8, with generators and relations as in 3.5.

EXAMPLE 6.3. In the dihedral group G we put $A = \mathrm{Gp}(a^2, ab)$, $X = \mathrm{Gp}(a^2)$, and $B = \mathrm{Gp}(b)$. Then A is of order 4, therefore normal in G, so that $A^G \cap B = A \cap B = E$: on the other hand B^G is clearly generated by b and $[a, b] = a^2$, so that $B^G \cap A = \mathrm{Gp}(a^2) = X$. Hence G is a linked product of A and B with kernels X and E, which was what we wanted.

We saw in section 4 (corollary 4.3) that if X is a perfect group, $X' = X$, the wreath product $X \mathrm{wr} B$ is a linked product of X and B with kernels X and E, for arbitrary B. The wreath product provides us with some further instances of unsymmetrical linked products:

THEOREM 6.4. *If X is a divisible abelian group, and B is arbitrary, then there exists a linked product of X and B with kernels X and E.*

This is an immediate consequence of a more precise statement, obtained with the aid of lemma 2.10:

THEOREM 6.5. *If X is an abelian group and every element possesses an n-th root for some fixed integer $n > 1$, and B is any group possessing an element of order n, or of infinite order, then there exists a linked product of X and B with kernels X and E.*

Proof. 1. Suppose $b \in B$ is of order n, and let $W = X \mathrm{wr} B$. By lemma 2.10 (i), the subset $\hat{X}$ consisting of all elements

$$f = x_e^{-1} x_b 1_{b^2} \ldots 1_{b^{n-1}}$$

is a subgroup isomorphic with X. We put $G = \mathrm{Gp}(\hat{X}, B)$.

Then $\hat{X}^W \cap B = E$, so that a fortiori $\hat{X}^G \cap B = E$. To see that $B^G \geqq \hat{X}$, we form the product $\prod_{k=0}^{n-1} b^{-k} f b^k$; an easy calculation proves this to be the unit element. Moreover, as f commutes with each conjugate $b^{-k} f b^k$, it follows that

$$\prod_{k=1}^{n-1} [f, b^k] = f^{-(n-1)} \prod_{k=1}^{n-1} b^{-k} f b^k;$$

hence

$$\prod_{k=1}^{n-1} [f, b^k] = f^{-(n-1)} \cdot f^{-1} = f^{-n}.$$

Therefore $[\hat{X}, B]$ contains all elements f^{-n} of $\hat{X}$, and therefore the whole of $\hat{X}$ itself. Since $\hat{X}$ is isomorphic with X, this means that G provides a linked product of X and B with kernels X and E.

2. If $b \in B$ has infinite order, we use the unrestricted wreath product $W = X \operatorname{Wr} B$ instead. The proof then is exactly as before, using the subgroup provided by lemma 2.10 (ii) this time.

Amongst other obvious consequences we note in particular:

COROLLARY 6.6. *If X and B are finite cycles of coprime orders, or if X is a finite and B an infinite cycle, then a linked product of X and B with kernels X and E exists; it can be taken finite when X and B are finite.*

This corollary does not even deal with all cases of pairs of finite cycles. Moreover, only some cases where B is of order 2, can be dealt with by the use of symmetric or alternating groups: the reason of course is that unsymmetrical linked products can never be simple.

However, BRITTON's theorem again applies.

LEMMA 6.7. *Let P be the free product $X * B$, where X is cyclic generated by x, and B is cyclic generated by b; let ω be the word obtained by reducing the following element of P to its cyclically reduced form:*

1. $x \cdot \prod_{k=2}^{5} [x^k, b]$ *if* $|b| > 2$, $|x| > 10$,
2. $x \cdot \prod_{k=2}^{11} [x^k, b]$ *if* $|b| = 2$, $|x| > 22$,
3. $x \cdot \prod_{k=1}^{4} [x, b^k]$ *if* $|b| > 8$, $|x| > 2$,
4. $x \cdot \prod_{k=1}^{10} [x, b^k]$ *if* $|b| > 20$, $|x| = 2$.

If Ω is the set consisting of the one element ω, then it satisfies the assumption 2.11 *of Britton's theorem* 2.12 [cf. footnote [4])].

Again we omit the check. The lemma leads easily to the following result:

THEOREM 6.8. *A linked product of the cyclic groups X and B with kernels X and E exists provided that the orders of X and B satisfy the restrictions of lemma* 6.7.

Proof. By BRITTON's result, the group $G = P/\Omega^P$ is generated by isomorphic copies of X and B which intersect trivially in G. The relation $\omega = 1$ is of the form

$$x = f(x, b)$$

with $f(x, b) \in [X, B]$; therefore $X \leqq [B, X]$ in G, and so $B^G \geqq X$. To show that $X^G \cap B = E$ in G, we need only show that adding the relation $x = 1$ to G does not affect B – in other words, $G/X^G \cong B$. But

$$G/X^G = P/\{\Omega, x\}^P = P/X^P \cong B,$$

since $\omega = 1$ is a consequence of $x = 1$, that is, $\Omega^P \leqq X^P$. This completes the proof of the theorem.

As in the case of lemmas 5.5 and 5.6, so lemma 6.7 can be modified to cover the case of X being an infinite cycle and B arbitrary, and the other way round, using the elements 1. and 2. of lemma 6.7 in the first case, but the elements 3. and 4. in the second case. This leads to:

THEOREM 6.9. *A linked product of groups X and B with kernels X and E exists whenever one of the groups is an infinite cycle, and the other arbitrary.*

As before, *this can be extended further to cover the case of one group being arbitrary and the other a group that can be generated by non-intersecting cycles of not too small orders.* But again we see no point in going into details, since we have no hope of attaining the general solution by this method.

References

[1] GOLOVIN, O. N.: Nilpotent products of groups. Mat. Sbornik **27**, 427–454 (1950).— Amer. Math. Soc. Transl. (2. Ser.) **2**, 89–115 (1956). – [2] BRITTON, J. L.: Solution of the word problem for certain types of groups II. Proc. Glasgow Math. Ass. **3**, 68–90 (1957). – [3] NEUMANN, B. H., and HANNA NEUMANN: Embedding theorems for groups. J. London Math. Soc. **34**, 465—479 (1959). – [4] NEUMANN, B. H.: An Essay on Free Products of Groups with Amalgamations. Phil. Trans. Roy. Soc. A **246**, 503–554 (1954). – [5] WIELANDT, H.: Einbettung zweier Gruppen in eine einfache Gruppe. Math. Z. **73**, 20—21 (1960).

Department of Mathematics, The Manchester College of Science and Technology, Manchester 1 (England)

Department of Mathematics, University College, Keele, Staffs. (England)

(Eingegangen am 9. Oktober 1959)

WIELANDT, H.
Math. Zeitschr. 73, 20–21 (1960)

Einbettung zweier Gruppen in eine einfache Gruppe

Von
HELMUT WIELANDT

HANNA NEUMANN und JAMES WIEGOLD [*1*, p. 2] haben die folgende Frage aufgeworfen: Wann kann man zwei gegebene Gruppen $\mathfrak{A}$, $\mathfrak{B}$ derart in eine einfache Gruppe $\mathfrak{G}$ einbetten, daß $\mathfrak{A}$ und $\mathfrak{B}$ nur das neutrale Element gemeinsam haben und die ganze Gruppe $\mathfrak{G}$ erzeugen? Dabei sind die Fälle ohne Interesse, in denen eine der beiden Ordnungen a, b gleich 1 ist oder $a=b=2$ ist; im letzten Fall ist das Erzeugnis von $\mathfrak{A}$ und $\mathfrak{B}$ stets eine Diedergruppe, also nicht einfach. Die genannten Autoren vermuten, daß die gewünschte Einbettung in allen anderen Fällen möglich ist. Diese Vermutung wird im folgenden für endliche Gruppen bestätigt, für unendliche bleibt sie offen.

SATZ. *Gegeben seien zwei endliche Gruppen $\mathfrak{A}$, $\mathfrak{B}$ der Ordnungen a, b mit $2 \leqq a \leqq b$, $4 < ab$. Dann läßt sich die alternierende Permutationsgruppe $\mathfrak{A}_n$ eines geeigneten Grades n mit $5 \leqq n < 2ab$ durch zwei Untergruppen erzeugen, die zu $\mathfrak{A}$, $\mathfrak{B}$ isomorph sind und nur die identische Permutation E gemeinsam haben.*

BEWEIS. Hat b den kleinsten möglichen Wert 3, so kommt man mit $n=5$ aus. Denn die Gruppe $\mathfrak{A}_5$ läßt sich sowohl durch

$$A=(1\,2)(4\,5), \qquad B=(2\,3\,4) \qquad (a=2)$$

wie durch

$$A=(1\,2\,3), \qquad B=(3\,4\,5) \qquad (a=3)$$

erzeugen. Weiterhin können wir $b \geqq 4$ annehmen.

Wir setzen $n=2(a-1)b+1$; dann ist $9 \leqq n < 2ab$. Wir wählen eine Menge Ω von n zu permutierenden Objekten („Ziffern") und bezeichnen diese mit

$$\begin{array}{llll} z_{11} & z_{12} & \cdots & z_{1b} \\ \cdot & \cdot & \cdots & \cdot \\ z_{a-1\,1} & z_{a-1\,2} & \cdots & z_{a-1\,b} \\ \\ z_{a1} & z_{a2} & \cdots & z_{ab} \\ \cdot & \cdot & \cdots & \cdot \\ z_{2a-2\,1} & z_{2a-2\,2} & \cdots & z_{2a-2\,b} \\ & z. & & \end{array}$$

Wir wählen eine zu $\mathfrak{B}$ isomorphe Permutationsgruppe auf Ω, welche die Ziffer z fest läßt und die übrigen Ziffern derart vertauscht, daß sie in ihren Zeilen bleiben und daß die b Spalten der Matrix (z_{ik}) entsprechend der regulären

Darstellung von $\mathfrak{B}$ vertauscht werden. Wir bezeichnen diese zu $\mathfrak{B}$ isomorphe Permutationsgruppe der Einfachheit halber ebenfalls mit $\mathfrak{B}$ und wählen in ihr irgendein Element $B \neq E$. Da B keine Spalte in sich überführt und da $b \geqq 4$ ist, gibt es in der Matrix (z_{ik}) ein Paar von Spalten, welches fremd ist zu dem Bildpaar, in das es bei Anwendung von B übergeht. Wir können also bei passender Bezeichnung annehmen, daß B die erste Spalte in die dritte überführt, und die zweite in die vierte.

Nun wählen wir eine zu $\mathfrak{A}$ isomorphe und weiterhin ebenfalls mit $\mathfrak{A}$ bezeichnete Permutationsgruppe auf Ω, welche die a Ziffern $z_{11}, \ldots, z_{a1}$ gemäß der regulären Darstellung von $\mathfrak{A}$ permutiert, das Gleiche mit den a Ziffern $z_{a2}, \ldots, z_{2a-22}, z$ tut und alle übrigen Ziffern einzeln fest läßt. In $\mathfrak{A}$ wählen wir ein beliebiges Element $A \neq E$.

Wir bilden die von $\mathfrak{A}$ und $\mathfrak{B}$ erzeugte Permutationsgruppe $\mathfrak{G}$. Um zu zeigen, daß $\mathfrak{G}$ die alternierende Gruppe $\mathfrak{A}_n$ auf Ω ist, genügt es nach einem bekannten Satz [2, p. 48], die folgenden drei Eigenschaften von $\mathfrak{G}$ nachzuprüfen: $\mathfrak{G} \leqq \mathfrak{A}_n$, $\mathfrak{G}$ primitiv, $\mathfrak{G}$ enthält einen Zyklus C des Grades 3.

a) Jede in $\mathfrak{A}$ oder $\mathfrak{B}$ auftretende Permutation P ist gerade. Denn in der Zyklenzerlegung von P kommen Zyklen eines bestimmten Grades stets in gerader Anzahl vor (sie ist durch 2 teilbar für $\mathfrak{A}$, durch $2a-2$ für $\mathfrak{B}$).

b) Nach Konstruktion ist $\mathfrak{G}$ transitiv auf Ω. Wäre $\mathfrak{G}$ imprimitiv, so gäbe es in Ω eine echte Teilmenge $\omega = \{z, z_{ik}, \ldots\}$ derart, daß aus $G \in \mathfrak{G}$ und $\omega^G \cap \omega \neq 0$ stets $\omega^G = \omega$ folgt (ω^G bezeichnet das Bild von ω nach Anwendung von G). Da $z^{\mathfrak{B}} = z$ ist, ergibt sich $\omega^{\mathfrak{B}} = \omega$; insbesondere ist $z_{ib} \in \omega$. Da $z_{ib}^{\mathfrak{A}} = z_{ib}$ ist, ergibt sich $\omega^{\mathfrak{A}} = \omega$. Hieraus folgt $\omega^{\mathfrak{G}} = \omega \neq \Omega$, im Widerspruch zur Transitivität von $\mathfrak{G}$.

c) Aus den gewählten Elementen A, B bilden wir zunächst $B^{-1}AB = D$. Da A genau die Ziffern $z_{11}, \ldots, z_{a1}, z_{a2}, \ldots, z_{2a-22}, z$ versetzt und da diese Ziffern von B in $z_{13}, \ldots, z_{a3}, z_{a4}, \ldots, z_{2a-24}, z$ übergeführt werden, versetzen A und D nur eine einzige Ziffer gemeinsam, nämlich z. Daher ist der Kommutator $A^{-1}D^{-1}AD = C$ ein Zyklus des Grades 3. Damit ist der Beweis beendet.

Literatur

[1] Neumann, H., and J. Wiegold: Linked products and linked embeddings of groups. Math. Z. 73, 1–19 (1960). — [2] Séguier, J.-A. de: Groupes de substitutions. Paris 1912.

Tübingen, Mathematisches Institut der Universität

(Eingegangen am 15. Oktober 1959)

SCHÖNHAGE, A.
Math. Zeitschr. 73, 22–44 (1960)

Über das Wachstum zusammengesetzter Funktionen

Von
ARNOLD SCHÖNHAGE

Inhalt

Seite
Einleitung 22
1. (i, k)-Wachstum als Verallgemeinerung der Ordnung 24
11. (i, k)-Wachstum, Wachstumsklassen 24
12. Das Wachstum von $f+g$, fg, f' 26
13. Koeffizientenabhängigkeit des Wachstums 28
14. Allgemeiner Wachstumsvergleich 33
2. Das Wachstum zusammengesetzter Funktionen 35
21. Multiplikationssatz 35
22. Beispiele 38
23. Verallgemeinerung eines Satzes von PÓLYA 41
24. Anwendungen auf die Funktionalgleichung $f(f(z)) = F(z)$ und verwandte Fragen 42
Literatur 43

Einleitung

Unter der Zusammensetzung von zwei ganzen Funktionen $f(z)$ und $g(z)$ versteht man die Bildung der (ganzen) Funktion

$$h(z) = f\big(g(z)\big). \tag{1}$$

f und g sollen Komponenten von h genannt werden. Bezüglich der Zusammensetzung bildet die Menge der ganzen Funktionen eine (nicht kommutative) Halbgruppe. Diese Operation ist aber von den arithmetischen Verknüpfungen $f+g$ und fg wesentlich verschieden. Während dort nur eine „stellenweise" Abhängigkeit vorliegt, ist hier der Abbildungscharakter der Komponenten von entscheidender Bedeutung. So lassen sich auf dem Wege über die Potenzreihen nur schwer Resultate gewinnen. Es ist aber nach all den bisher bekannten Eigenschaften der ganzen Funktionen zu erwarten, daß auch für ihre Zusammensetzung strenge Gesetzmäßigkeiten bestehen.

Für den Spezialfall der Iterierten einer Funktion $f(z)$, die rekursiv durch

$$f_0(z) = z, \qquad f_1(z) = f(z), \qquad f_{n+1}(z) = f\big(f_n(z)\big) \tag{2}$$

definiert werden, liegen schon ausgedehnte Ergebnisse vor. Insbesondere wurde ihr infinites Verhalten, die Interpolation bezüglich des Parameters n und die damit in engstem Zusammenhang stehende Schrödersche Funktionalgleichung

$$S\big(f(z)\big) = a\,S(z) \tag{3}$$

behandelt (vgl. [1] bis [19]). Weiter fand in jüngerer Zeit speziell die Funktionalgleichung

$$f(f(z)) = F(z) \tag{4}$$

reges Interesse ([22]—[28]).

Über die Zusammensetzung (1) in voller Allgemeinheit ist jedoch weniger bekannt. RITT [20] und JACOBSTHAL [21] beschränken sich auf Polynome. PÓLYA [29] behandelt den Fall, daß h von endlicher Ordnung ist (vgl. 23.). ROSENBLOOM [22] diskutiert die Zusammensetzung von Funktionen mit endlich vielen Fixpunkten. Über die Zusammensetzung von Funktionen kleiner Ordnung schließlich erzielt BAKER [25] eine Reihe von interessanten Einzelresultaten.

Ziel der vorliegenden Arbeit ist es, den Zusammenhang zu untersuchen, der zwischen der Zusammensetzung und dem Wachstum der Funktionen besteht. Das Wachstum einer Funktion $f(z)$ wird dabei wie üblich durch

$$M(r,f) = \max_{|z|=r} \{|f(z)|\} \tag{5}$$

charakterisiert. Es zeigt sich jedoch, daß der gewöhnliche Ordnungsbegriff

$$\varrho(f) = \overline{\lim_{r\to\infty}} \left(\frac{\lg\lg M(r,f)}{\lg r}\right) \tag{6}$$

allein kein geeignetes Wachstumsmaß ist:

BAKER [24] gibt Funktionen f_1, f_2, f_3 an, für die

$$\varrho(f_1) = 0, \quad \varrho(f_1(f_1)) = 0; \tag{7a}$$

$$\varrho(f_2) = 0, \quad \varrho(f_2(f_2)) = 1; \quad \text{(vgl. 22.)} \tag{7b}$$

$$\varrho(f_3) = 0, \quad \varrho(f_3(f_3)) = \infty. \tag{7c}$$

Weiterhin haben Polynome; für die sich doch weit mehr aussagen läßt, sämtlich die Ordnung 0; aus $\varrho(f) > 0$, $\varrho(g) > 0$ folgt andererseits aber stets $\varrho(f(g)) = \infty$.

Die vorstehenden Beispiele zeigen die Notwendigkeit, ein differenzierteres Wachstumsmaß einzuführen. So wird im Abschnitt 1. — in natürlicher Erweiterung der Ordnung (6) — das (i, k)-Wachstum definiert und beschrieben. Bei diesem Wachstumsvergleich werden die Iterierten der Exponentialfunktion als Vergleichsfunktionen zugrunde gelegt. In 14. wird gezeigt, wie sich die Begriffsbildungen analog auch für andere Vergleichsfunktionen durchführen lassen, daß aber der Exponentialfunktion eine Sonderstellung zukommt, auf die wir uns hier beschränken wollen.

Im Abschnit 2. wird mit Hilfe eines Satzes von PÓLYA [29] als zentrales Ergebnis bewiesen, daß sich das Wachstum der Funktionen f und g bei der Zusammensetzung (1) im wesentlichen multipliziert (Multiplikationssatz). Ein sehr einfaches Beispiel dafür ist z. B. die Multiplikation der Grade bei der Zusammensetzung von Polynomen. — Danach finden in 22. die Bakerschen Beispiele (7) eine befriedigende Erklärung. Es ergeben sich weiter innerhalb

der Ordnung 0 abzählbar viele natürliche Wachstumsgrenzen, die bei Zusammensetzung nicht übersprungen werden. In 24. schließlich sollen die Anwendungsmöglichkeiten des Multiplikationssatzes an einigen spezielleren Problemen gezeigt werden.

1. (i,k)-Wachstum als Verallgemeinerung der Ordnung

Wir schreiben im folgenden, sofern Mißverständnisse ausgeschlossen sind, statt $M(r,f)$ kürzer $M(r)$. Weiter werden die (reellen) Iterierten von $\lg x$ und $\exp x$ gebraucht, entsprechend den Festsetzungen (2). Bei $\lg_k x$ soll stets $x > \exp_k 0$ angenommen werden, so daß also $\lg_k x > 0$. Bei negativem k ist die Umkehrfunktion gemeint, d.h. allgemein gilt

$$\lg_k x = \exp_{-k} x \qquad (k \text{ ganz}).$$

Es sollen gleich die wichtigsten hier benutzten Tatsachen über $\lg_k x$ zusammengestellt werden:

Aus $p_n \to \infty$, $q_n \to \infty$, $\frac{p_n}{q_n} \to c$ folgt $(k \geqq 1)$

(8a) $$\frac{\lg_k p_n}{q_n} \to 0 \quad \text{für} \quad c < \infty,$$

(8b) $$\frac{p_n}{\lg_k q_n} \to \infty \quad \text{für} \quad c > 0,$$

(8c) $$\frac{\lg_k p_n}{\lg_k q_n} \to 1 \quad \text{für} \quad 0 < c < \infty.$$

Für $k \geqq 0$ gelten die Abschätzungen

(9) $$\lg_k(a+b) \leqq \lg_k a + \lg_k b, \qquad (a, b \geqq \exp_{k-1} 2),$$

(10a) $$\lg_k(a+b) \leqq \lg_k a + b,$$

(10b) $$\lg_k(a-b) \geqq \lg_k a - b \qquad (b \geqq 0).$$

11. (i,k)-Wachstum, Wachstumsklassen

In Erweiterung des Ordnungsbegriffes, den wir auch weiterhin nur im alten Sinne (6) gebrauchen werden, definieren wir nunmehr als das obere bzw. untere (i,k)-Wachstum einer ganzen (nicht konstanten) Funktion $f(z)$:

(11a) $$\overline{W}_{i,k}(f) = \overline{\lim_{r\to\infty}} \left(\frac{\lg_{k+i} M(r)}{\lg_k r} \right),$$

(11b) $$\underline{W}_{i,k}(f) = \underline{\lim_{r\to\infty}} \left(\frac{\lg_{k+i} M(r)}{\lg_k r} \right), \qquad (i,k = 0,1,\ldots).$$

Wir setzen für $f(z) \equiv c$ formal $\overline{W}_{i,k}(f) = \underline{W}_{i,k}(f) = 0$, wollen diesen trivialen Fall aber in Zukunft generell ausschließen. Wenn $\overline{W}_{i,k}(f) = \underline{W}_{i,k}(f)$, nennen wir f von regulärem (i,k)-Wachstum und schreiben schlechthin $W_{i,k}(f)$. Ein hinreichendes Kriterium hierfür wird in 13. gegeben.

Weiter führen wir die Mengen

(12a) $$H_{i,k} = \{f(z) \mid 0 < \overline{W}_{i,k}(f) < \infty\}$$

ein (für $g \notin H_{i,k}$ ist also $\overline{W}_{i,k}(g) = 0$ oder $= \infty$). Wegen (8c) gilt dann $H_{i,k} \subset H_{i,k+1}$. Für festes i bilden die $H_{i,k}$ also ein abzählbares Hüllensystem, und man erhält die Wachstumsklassen

$$H_i = \bigcup_{k=0}^{\infty} H_{i,k} \qquad (i = 0, 1, \ldots). \tag{12b}$$

Wegen (8a) und (8b) ist $H_i \cap H_j$ für $i \neq j$ leer. Um eine vollständige Klassifikation der ganzen Funktionen zu bekommen, führen wir schließlich noch Zwischenklassen ein:

$$Z_i = \{f(z) \mid \overline{W}_{i,k}(f) = \infty, \ \overline{W}_{i+1,k}(f) = 0;\ k = 0, 1, \ldots\}, \tag{12c}$$

$$Z_\infty = \{f(z) \mid \overline{W}_{i,0}(f) = \infty, \quad i = 0, 1, \ldots\}. \tag{12d}$$

Daß es solche Funktionen gibt, diese Klassen also nicht leer sind, wird in 22. gezeigt.

Einige der $H_{i,k}$ sind sofort zu überschauen:

$H_{1,1}$: Funktionen endlicher positiver Ordnung, denn

$$\overline{W}_{1,1}(f) = \varrho(f).$$

$H_{1,0}$: Funktionen der Ordnung 1 vom Normaltyp $\overline{W}_{1,0}(f)$.

$H_{0,0}$: Lineare Funktionen $f(z) = az + b$, wobei $W_{0,0}(f) = |a|$.

$H_{0,1}$: Polynome $P_n(z)$, $W_{0,1}(P_n) = n$.

Hier zeigt sich, daß stets $\underline{W}_{0,0} = \overline{W}_{0,0}$ und $\underline{W}_{0,1} = \overline{W}_{0,1}$, denn bei transzendenten Funktionen f ist auch $\underline{W}_{0,1}(f) = \infty$, weil $\lg M(r)$ eine konvexe Funktion von $\lg r$ ist (Hadamardscher Dreikreisesatz).

Für $(i, k) \neq (0, 0), (1, 0)$ kann das (i, k)-Wachstum statt durch $M(r)$ auch mittels der charakteristischen Funktion $T(r)$ (vgl. [33]) ausgedrückt werden: *Es gilt (außer für die oben genannten Fälle)*

$$\overline{W}_{i,k}(f) = \overline{\lim_{r \to \infty}} \left(\frac{\lg_{k+i-1} T(r)}{\lg_k r} \right), \tag{13a}$$

$$\underline{W}_{i,k}(f) = \underline{\lim_{r \to \infty}} \left(\frac{\lg_{k+i-1} T(r)}{\lg_k r} \right). \tag{13b}$$

Zum Beweise verwenden wir die für ganze Funktionen geltende Ungleichung

$$T(r) \leqq \lg M(r) \leqq \frac{R + r}{R - r} T(R) \qquad (0 < r < R). \tag{14}$$

Für $k \geqq 1$, $i + k \geqq 2$ folgt aus ihr (unter Berücksichtigung von (10))

$$\frac{\lg_{k+i-1} T(r)}{\lg_k r} \leqq \frac{\lg_{k+i} M(r)}{\lg_k r} \leqq \frac{\lg\left(\frac{R + r}{R - r}\right) + \lg_{k+i-1} T(R)}{\lg_k R - \lg\left(\frac{R}{r}\right)} \tag{15a}$$

und durch Grenzübergang $r \to \infty$ (bei fest gewähltem Verhältnis $\frac{R}{r}$) (13).

Für $k=1$, $i=0$ ist im Falle $f=P_n(z)$ $T(r)=n\lg r+O(1)$, also

$$\lim_{r\to\infty}\left(\frac{T(r)}{\lg r}\right)=n=W_{0,1}(f).$$

Wenn f transzendent ist, also $\frac{\lg M(r)}{\lg r}\to\infty$, setze man in (14) etwa $R=2r$ und erhält

$$\frac{\lg M(r)}{\lg r}\leqq\frac{3\,T(2r)}{\lg(2r)-\lg 2},\quad\text{also auch}\quad\frac{T(R)}{\lg R}\to\infty.$$

Im Falle $k=0$, $i\geqq 2$ schließlich hat man statt (15a) auf der rechten Seite

$$\frac{\lg_i M(r)}{r}\leqq\frac{\lg\left(\frac{R+r}{R-r}\right)+\lg_{i-1}T(R)}{R}\cdot\frac{R}{r}. \tag{15b}$$

Hier liefert der Grenzübergang $r\to\infty$ mit $R=r\left(1+\frac{1}{m}\right)$ (für jedes feste m) die Behauptung.

12. Das Wachstum von $f+g$, fg und f'

In diesem wie im folgenden Abschnitt sollen bekannte allgemeine Sätze über die Ordnung auf das (i,k)-Wachstum übertragen werden. Für die Summe und das Produkt von ganzen Funktionen gilt

SATZ 1:

$$\left.\begin{aligned}&\overline{W}_{i,k}(f+g)\\&\overline{W}_{i,k}(fg)\end{aligned}\right\}\leqq\max\{\overline{W}_{i,k}(f);\ \overline{W}_{i,k}(g)\}\ \text{für}\ \begin{cases}i+k\geqq 1,\\ i+k\geqq 2.\end{cases}\qquad\begin{aligned}&\text{(16a)}\\&\text{(16b)}\end{aligned}$$

Falls $\overline{W}_{i,k}(f)\neq\overline{W}_{i,k}(g)$, dann steht in (16) *das Gleichheitszeichen.*

Zum Beweise von (16a) dient die Ungleichung

$$M(r,f)-M(r,g)\leqq M(r,f+g)\leqq M(r,f)+M(r,g). \tag{17a}$$

Wir setzen $\overline{W}_{i,k}(f)=a$, $\overline{W}_{i,k}(g)=b$, und es sei $\infty>a\geqq b$ (für $a=\infty$ ist (16a) klar). Dann folgt aus der Definition (11a) für $r\geqq r_0(\varepsilon)$

$$M(r,f)<\exp_{k+i}[(a+\varepsilon)\lg_k r],$$
$$M(r,g)<\exp_{k+i}[(b+\varepsilon)\lg_k r],$$

also

$$M(r,f+g)\leqq M(r,f)+M(r,g)<2\exp_{k+i}[(a+\varepsilon)\lg_k r]$$

und wegen $i+k\geqq 1$ (und (10a))

$$\frac{\lg_{k+i}M(r,f+g)}{\lg_k r}<\frac{\lg 2}{\lg_k r}+a+\varepsilon,$$

$$\overline{W}_{i,k}(f+g)\leqq a+\varepsilon\qquad\text{für alle}\qquad\varepsilon>0.$$

Nunmehr sei $b<a\leqq\infty$. Man wähle $\varepsilon>0$ mit $a-\varepsilon>b+\varepsilon$ (falls $a=\infty$, setze man $1/\varepsilon$ statt $a-\varepsilon$). Dann gilt für gewisse $r_m\to\infty$ von einem $m_0(\varepsilon)$ an

$$M(r_m,f)>\exp_{k+i}[(a-\varepsilon)\lg_k r_m]>2\exp_{k+i}[(b+\varepsilon)\lg_k r_m]>2M(r_m,g),$$

also

$$2M(r_m, f+g) \geqq 2M(r_m, f) - 2M(r_m, g) > M(r_m, f),$$

$$\frac{\lg 2 + \lg_{k+i} M(r_m, f+g)}{\lg_k r_m} > \frac{\lg_{k+i} M(r_m, f)}{\lg_k r_m} > a - \varepsilon$$

und schließlich $\overline{W}_{i,k}(f+g) \geqq a - \varepsilon$, womit auch der Zusatz in Satz 1 für (16a) bewiesen ist.

Um (16b) zu zeigen, wenden wir NEVANLINNAs 1. Hauptsatz über meromorphe Funktionen an:

$$T(r, f) \leqq T(r, fg) + T\left(r, \frac{1}{g}\right) = T(r, fg) + T(r, g) + O(1).$$

Damit haben wir, in Analogie zu (17a),

$$T(r, f) - T(r, g) + O(1) \leqq T(r, fg) \leqq T(r, f) + T(r, g). \tag{17b}$$

Da für (16b) $i+k \geqq 2$ vorausgesetzt wird, verläuft der Beweis für fg unter Verwendung von (13) nunmehr in gleicher Weise wie für $f+g$, indem man überall $\lg M(r)$ durch $T(r)$ ersetzt.

Die Verallgemeinerung von $\varrho(f) = \varrho(f')$ gibt

SATZ 2. *Für* $(i, k) \neq (0, 0), (0, 1)$ *gilt*

$$\overline{W}_{i,k}(f') = \overline{W}_{i,k}(f), \tag{18a}$$

$$\underline{W}_{i,k}(f') = \underline{W}_{i,k}(f). \tag{18b}$$

Wir verwenden die Ungleichung

$$\frac{M(r, f) - |f(0)|}{r} \leqq M(r, f') \leqq \frac{M(R, f)}{R - r} \qquad (0 < r < R) \tag{19}$$

(TITCHMARSH, Theory of functions, p. 265). Weiter kann wegen $(i, k) \neq (0, 0), (0, 1)$ vorausgesetzt werden, daß f transzendent ist, also

$$\frac{\lg M(r, f)}{\lg r} \to \infty. \tag{20}$$

Dann folgt für $i + k \geqq 1$ aus der linken Seite von (19)

$$\lg M(r, f) - \lg r + O(1) \leqq \lg M(r, f'),$$

für $r \geqq r_0(\varepsilon)$ nach (20) also

$$(1 - \varepsilon) \lg M(r, f) < \lg M(r, f')$$

und

$$(1 - \varepsilon) \frac{\lg_{k+i} M(r, f)}{\lg_k r} < \frac{\lg_{k+i} M(r, f')}{\lg_k r}. \tag{21}$$

Setzt man auf der rechten Seite von (19) $R = (1+\varepsilon) r$, dann ist für $r \geqq r_1(\varepsilon)$

$$M(r, f') \leqq \frac{M(R, f)}{\varepsilon r} < M(R, f),$$

$$\frac{\lg_{k+i} M(r, f')}{\lg_k r} < \frac{\lg_{k+i} M(R, f)}{\lg_k R} \cdot \frac{\lg_k (1+\varepsilon) r}{\lg_k r}. \tag{22}$$

(21) und (22) ergeben im Grenzübergang $r \to \infty$, $\varepsilon \to 0$ die Behauptung (18).

13. Koeffizientenabhängigkeit des Wachstums

Die Ordnung einer Funktion

$$f(z) = \sum a_n z^n$$

ist bekanntlich durch das infinite Verhalten der $|a_n|$ bestimmt:

$$\overline{W}_{1,1}(f) = \overline{\lim_{n\to\infty}} \left(\frac{n \lg n}{\lg\left(\frac{1}{|a_n|}\right)} \right). \tag{23}$$

Eine ähnliche Abhängigkeit besteht auch für den Normaltyp der Ordnung 1:

$$\overline{W}_{1,0}(f) = \overline{\lim_{n\to\infty}} \left(\frac{n}{e} \sqrt[n]{|a_n|} \right) = \overline{\lim_{n\to\infty}} \left(\sqrt[n]{n!\,|a_n|} \right), \tag{24}$$

(vgl. PRINGSHEIM [32]). (23) und (24) lassen die einheitliche Darstellung

$$\overline{W}_{1,k}(f) = \overline{\lim_{n\to\infty}} \left(\frac{\lg_k \sqrt[n]{n!}}{\lg_k \sqrt[n]{\frac{1}{|a_n|}}} \right) \quad (k = 0, 1) \tag{25}$$

zu. Wir werden zeigen, daß (25) für alle k zutrifft. Beachtet man weiter, daß $n!$ der reziproke Koeffizient von e^z ist, dann liegt nahe, daß für $i > 1$ die Koeffizienten von

$$\exp_i z = \sum b_{i,n} z^n \qquad (b_{i,n} > 0) \tag{26}$$

die allgemeine Koeffizientenabhängigkeit des Wachstums bestimmen. Wir untersuchen deshalb zunächst die $b_{i,n}$.

Nach der Stirlingschen Formel ist

$$\sqrt[n]{\frac{1}{n!}} \sim \frac{e}{n} \qquad \left(p_n \sim q_n \text{ im Sinne von } \frac{p_n}{q_n} \to 1\right). \tag{27}$$

Um das asymptotische Verhalten der $\sqrt[n]{b_{i,n}}$ für beliebiges $i \geqq 1$ zu beschreiben, führen wir von n und i abhängige Zahlen $u_{i,n}$ ein, die durch die Gleichung

$$n = \prod_{j=0}^{i-1} \lg_j u_{i,n} \tag{28}$$

eindeutig bestimmt sind ($n \geqq n_i$, so daß $u_{i,n} \geqq \exp_i 1$). Es ist $u_{1,n} = n$, für $i \geqq 2$ aber lassen sich die $u_{i,n}$ nicht explizit angeben. Aus (8) und (28) folgt

$$\frac{\lg u_{1,n}}{\lg n} \to 1 \tag{29a}$$

und für $i \geqq 2$

$$\frac{u_{i,n}}{n} \to 0. \tag{29b}$$

Nunmehr beweisen wir

SATZ 3:

$$\sqrt[n]{b_{i,n}} \sim \frac{\exp\left(\frac{u_{i,n}}{n}\right)}{\lg_{i-1} u_{i,n}}. \tag{30}$$

Für $i=1$ geht (30) in (27) über; für $i\geqq 2$ hat man wegen (29) vereinfacht

$$\sqrt[n]{b_{i,n}} \sim \frac{1}{\lg_{i-1} n}. \tag{31}$$

Wir zeigen zuerst durch vollständige Induktion über i, daß

$$b_{i,n} > K_{i,n} \exp\left\{u_{i,n} - \prod_{j=0}^{i} \lg_j u_{i,n}\right\} \quad (n \geqq n_i), \tag{32}$$

wobei

$$\sqrt[n]{K_{i,n}} \to 1 \quad \text{für} \quad n \to \infty.$$

Für $i=1$ folgt (32) aus (27). Also sei jetzt (32) für i vorausgesetzt. Wir bilden

$$\exp_{i+1} z = \exp_i e^z = \sum_{n=0}^{\infty} b_{i,n} e^{nz} = \sum_{n,m=0}^{\infty} b_{i,n} \cdot \frac{n^m}{m!} z^m.$$

Es ist also

$$b_{i+1,m} = \frac{1}{m!} \sum_{n=0}^{\infty} b_{i,n} n^m > \frac{1}{m!} \sum_{n=n_i}^{\infty} K_{i,n} \exp\left\{u_{i,n} - \prod_{j=0}^{i} \lg_j u_{i,n}\right\} \left(\prod_{j=0}^{i-1} \lg_j u_{i,n}\right)^m. \tag{33}$$

Um ein möglichst großes Glied der Reihe zu bestimmen, suchen wir den Extremwert der Hilfsfunktion

$$h(u) = \exp\left(u - \prod_{j=0}^{i} \lg_j u\right) \left(\prod_{j=0}^{i-1} \lg_j u\right)^m;$$

$$\lg h(u) = u - \prod_{j=0}^{i} \lg_j u + m \sum_{j=1}^{i} \lg_j u. \tag{34}$$

$$\frac{h'(u)}{h(u)} = 1 - \left(\prod_{j=0}^{i} \lg_j u\right) \sum_{j=0}^{i} \left(\prod_{l=0}^{j} \frac{1}{\lg_l u}\right) + m \sum_{j=0}^{i-1} \left(\prod_{l=0}^{j} \frac{1}{\lg_l u}\right) = 0$$

ergibt für u_{extr} die Gleichung

$$\prod_{j=0}^{i} \lg_j u = m, \quad \text{also} \quad u_{\text{extr}} = u_{i+1,m}.$$

Wir verkleinern in (33) weiter, indem wir statt der Reihe nur das Glied mit dem Index

$$n_m = \max\{n \mid u_{i,n} \leqq u_{i+1,m}\} \tag{35}$$

setzen (wobei $m \geqq m_i$, damit $n_m \geqq n_i$. Abkürzend schreiben wir $u_{i,n_m} = u_n$, $u_{i,n_m+1} = u_{n+1}$ und $u_{i+1,m} = u_m$):

$$b_{i+1,m} > \frac{1}{m!} K_{i,n} h(u_n) > K_{1,m} \frac{e^m}{m^m} K_{i,n} \cdot \frac{h(u_n)}{h(u_m)} \cdot h(u_m). \tag{36}$$

Zunächst ist

$$\frac{e^m}{m^m} h(u_m) = \frac{e^m}{m^m} \exp(u_m - m) \left(\frac{m}{\lg_i u_m}\right)^m$$

$$= \frac{\exp u_m}{(\lg_i u_m)^m} = \exp\left(u_m - \prod_{j=0}^{i+1} \lg_j u_m\right). \tag{37}$$

Weiter ist noch

$$K_{i+1,m} = K_{1,m} \cdot K_{i,n} \cdot \frac{h(u_n)}{h(u_m)}$$

zu diskutieren: $\sqrt[m]{K_{1,m}} \to 1$, wegen $n_m \leqq m$ aber auch $\sqrt[m]{K_{i,n}} \to 1$. Wegen (28) gilt $u_{n+1} - u_n < 1$, wegen (35) $u_n \leqq u_m < u_{n+1}$. Der Extremwert bei u_m kann wegen der Konvergenz der Reihen in (33) nur ein Maximum sein. Somit folgt

$$1 \leqq \frac{h(u_m)}{h(u_n)} < \exp(u_m - u_n)\left(\frac{n+1}{n}\right)^m < e\left(1 + \frac{1}{n_m}\right)^m.$$

Wegen $n_m \to \infty$ für $m \to \infty$ ergibt sich schließlich

$$\sqrt[m]{\frac{h(u_m)}{h(u_n)}} \to 1, \quad \text{also}$$

$$\sqrt[m]{K_{i+1,m}} \to 1. \tag{38}$$

Mit (37) und (38) ist der Induktionsschritt für (32) geführt. Um nun auch (30) bzw. (31) zu zeigen, wählen wir in

$$b_{i,n} r^n < \exp_i r \qquad (n \geqq n_i) \tag{39}$$

ein r_n, so daß $g(r) = r^{-n} \exp_i r$ minimal wird:

$$\lg g(r) = \exp_{i-1} r - n \lg r;$$

$$r \frac{g'(r)}{g(r)} = \prod_{j=0}^{i-1} \exp_j r - n = 0$$

wird wegen (28) gerade von $r_n = \lg_{i-1} u_{i,n}$ erfüllt. (39) lautet für $r = r_n$

$$b_{i,n} < \exp(u_{i,n} - n \lg r_n) = \exp\left(u_{i,n} - \prod_{j=0}^{i} \lg_j u_{i,n}\right),$$

wodurch in Verbindung mit (28) und (32) Satz 3 bewiesen ist.

Jetzt läßt sich die gesuchte Verallgemeinerung von (25) angeben:

SATZ 4. *Für $i \geqq 1$, $k \geqq 0$ gilt*

$$\overline{W}_{i,k}(f) = \overline{\lim_{n\to\infty}}\, Q_n, \tag{40a}$$

$$\underline{W}_{i,k}(f) \geqq \underline{\lim_{n\to\infty}}\, Q_n, \tag{40b}$$

$$Q_n = \frac{\lg_k \sqrt[n]{\frac{1}{b_{i,n}}}}{\lg_k \sqrt[n]{\frac{1}{|a_n|}}}$$

falls also $\overline{\lim}\, Q_n = \underline{\lim}\, Q_n$, *dann insbesondere*

$$W_{i,k}(f) = \lim_{n\to\infty} Q_n. \tag{40c}$$

Weiter läßt sich wegen Satz 3 und (8c) Q_n *in* (40) *durch* Q_n^* *ersetzen, wobei*

$$Q_n^* = \frac{n}{e} \sqrt[n]{|a_n|} \qquad \text{für} \quad (i,k) = (1,0), \tag{41a}$$

$$Q_n^* = \frac{\lg_{k+i-1} n}{\lg_k \sqrt[n]{\frac{1}{|a_n|}}} \qquad \text{für} \quad i + k \geqq 2. \tag{41b}$$

Beim Beweise wie für die Anwendung von Satz 4 ist die Darstellung (41) von großem Vorteil, da die $b_{i,n}$ selbst für $i \geqq 2$ nicht bekannt sind.

Daß $i \geqq 1$ keine willkürliche Einschränkung ist, zeigt sich schon daran, daß die obigen Grenzwertbetrachtungen bei linearen Funktionen und Polynomen versagen. Man kann die natürliche Ausnahmestellung des Falles $i = 0$ aber auch an der allgemeinen Darstellung (40) ablesen.

Einfache Beispiele wie etwa $f(z) = \sin z$ zeigen, daß in (40b) allgemein nicht das Gleichheitszeichen gilt.

(40c) schließlich ist ein wichtiges Kriterium dafür, daß f von regulärem (i, k)-Wachstum ist.

Beim Nachweis von (40a) können wir von dem bekannten Fall (24) absehen, also im folgenden $i + k \geqq 2$ voraussetzen und die Darstellung (41b) verwenden. Zuerst zeigen wir

$$\overline{\lim_{r \to \infty}} \left(\frac{\lg_{k+i} M(r)}{\lg_k r} \right) = C \geqq \overline{\lim_{n \to \infty}} \left(\frac{\lg_{k+i-1} n}{\lg_k \sqrt[n]{\frac{1}{|a_n|}}} \right). \tag{42}$$

Für $C = \infty$ ist (42) klar. Wir nehmen also $C < \infty$ an und setzen $C + \varepsilon = B$ $(\varepsilon > 0)$. Dann gilt für $r \geqq r_0(\varepsilon)$

$$M(r) < \exp_{k+i}^{*}(B \lg_k r).$$

Nach Cauchy ist $|a_n| r^n \leqq M(r)$, also

$$\sqrt[n]{\frac{1}{|a_n|}} > r [\exp_{k+i}(B \lg_k r)]^{-\frac{1}{n}}.$$

Wählt man (wir schreiben, da i fest ist, statt $u_{i,n}$ kürzer u_n)

$$r = \exp_k \left(\frac{1}{B} \lg_{k+i-1} u_n \right) \qquad (n \geqq n_0, \text{ so daß } r \geqq r_0),$$

dann folgt

$$\sqrt[n]{\frac{1}{|a_n|}} > \exp_k \left(\frac{1}{B} \lg_{k+i-1} u_n \right) \exp\left(- \frac{u_n}{n} \right) \tag{43}$$

und für $k \geqq 1$ mittels (10b)

$$\lg \sqrt[n]{\frac{1}{|a_n|}} > \exp_{k-1} \left(\frac{1}{B} \lg_{k+i-1} u_n \right) - \frac{u_n}{n},$$

$$\frac{\lg_k \sqrt[n]{\frac{1}{|a_n|}}}{\lg_{k+i-1} n} > \frac{1}{B} \cdot \frac{\lg_{k+i-1} u_n}{\lg_{k+i-1} n} - \frac{1}{\lg_{k+i-1} n},$$

wegen $i + k \geqq 2$, (29a) und (8c) also

$$\lim_{n \to \infty} \left(\frac{1}{Q_n^*} \right) \geqq \frac{1}{C + \varepsilon}. \tag{44}$$

Für $k = 0$, $i \geqq 2$ folgt (44) wegen (29b) direkt aus (43). (44) gilt für jedes $\varepsilon > 0$, womit (42) bewiesen ist.

Für (40a) ist nun noch die zweite Ungleichung

$$\overline{\lim_{n\to\infty}}\left(\frac{\lg_{k+i-1} n}{\lg_k \sqrt[n]{\frac{1}{|a_n|}}}\right) = C \geqq \overline{\lim_{r\to\infty}}\left(\frac{\lg_{k+i} M(r)}{\lg_k r}\right) \tag{45}$$

zu zeigen. Wieder sei $C<\infty$ und $C+\varepsilon=B$. Für $n\geqq n_0(\varepsilon)$ gilt dann

$$\sqrt[n]{\frac{1}{|a_n|}} > \exp_k\left(\frac{1}{B}\lg_{k+i-1} n\right) > 1,$$

$$|a_n| < \left[\exp_k\left(\frac{1}{B}\lg_{k+i-1} n\right)\right]^{-n} < 1.$$

Damit läßt sich für hinreichend großes r abschätzen:

$$M(r) \leqq \sum_{n=0}^{\infty} |a_n| r^n < r^{n_0} + \sum_{n=n_0}^{\infty} r^n \left[\exp_k\left(\frac{1}{B}\lg_{k+i-1} n\right)\right]^{-n}.$$

Wir zerlegen $\sum_{n_0}^{\infty} = \sum_{n_0}^{n_1} + \sum_{n_1+1}^{\infty}$, worin

$$n_1 = [\exp_{k+i-1}(B \lg_k \delta r)] \tag{46}$$

($\delta>1$ fest gewählt und $r\geqq r_0(\varepsilon)$, so daß $n_1\geqq n_0$).

$$\sum_{n=n_1+1}^{\infty} r^n \left[\exp_k\left(\frac{1}{B}\lg_{k+i-1} n\right)\right]^{-n} < \sum_{n=0}^{\infty} \frac{1}{\delta^n} = \frac{\delta}{\delta-1} = D.$$

$$\sum_{n=n_0}^{n_1} r^n \left[\exp_k\left(\frac{1}{B}\lg_{k+i-1} n\right)\right]^{-n} < n_1 r^{n_1}.$$

Somit haben wir

$$M(r) < r^{n_0} + n_1 r^{n_1} + D.$$

Die Anwendung von (9) und (10a) ergibt in Verbindung mit (46)

$$\lg M(r) < n_0 \lg r + D + \lg n_1 + n_1 \lg r,$$

$$\lg_2 M(r) < (\lg n_0 + 1)\lg_2 r + D + \exp_{k+i-3}(B \lg_k \delta r) + \exp_{k+i-2}(B \lg_k \delta r),$$

$$\frac{\lg_{k+i} M(r)}{\lg_k r} < \frac{O(\lg_{k+i} r)}{\lg_k r} + \frac{\lg B + \lg_{k+1} \delta r}{\lg_k r} + B\frac{\lg_k \delta r}{\lg_k r}. \tag{47}$$

Wegen $i\geqq 1$ und (8) folgt für $k\geqq 1$

$$\overline{W}_{i,k}(f) \leqq (C+\varepsilon). \tag{48}$$

Im Falle $k=0$ erhält man aus (47) $\overline{W}_{i,k}(f)\leqq(C+\varepsilon)\delta$ für jedes $\delta>1$, also ebenfalls (48). Aus (48) folgt (45), womit (40a) vollständig bewiesen ist.

(40b) zeigen wir zunächst für $i+k\geqq 2$:

$$\underline{\lim_{n\to\infty}}\left(\frac{\lg_{k+i-1} n}{\lg_k \sqrt[n]{\frac{1}{|a_n|}}}\right) = C \leqq \underline{\lim_{r\to\infty}}\left(\frac{\lg_{k+i} M(r)}{\lg_k r}\right). \tag{49}$$

Wir können $C>0$ annehmen und setzen $B=C-\varepsilon$ $(0<\varepsilon<C)$, falls $C<\infty$, $B=\frac{1}{\varepsilon}$, falls $C=\infty$. Für $n\geqq n_0(\varepsilon)$ folgt

$$\sqrt[n]{\frac{1}{|a_n|}}<\exp_k\left(\frac{1}{B}\lg_{k+i-1}n\right),$$

$$|a_n|>\left[\exp_k\left(\frac{1}{B}\lg_{k+i-1}n\right)\right]^{-n}, \tag{50}$$

also

$$M(r)\geqq|a_n|\,r^n>r^n\left[\exp_k\left(\frac{1}{B}\lg_{k+i-1}n\right)\right]^{-n}.$$

Wir wählen

$$n=[\exp_{k+i-1}(B\lg_k\delta r)]\qquad\left(\frac{1}{e}<\delta<1\right):$$

$$M(r)>\frac{1}{\delta^n},$$

$$\lg M(r)>n\lg\frac{1}{\delta}>[\exp_{k+i-1}(B\lg_k\delta r)-1]\lg\frac{1}{\delta},$$

$$\lg_2 M(r)>\exp_{k+i-2}(B\lg_k\delta r)-1+\lg_2\frac{1}{\delta},$$

$$\frac{\lg_{k+i}M(r)}{\lg_k r}>B\,\frac{\lg_k\delta r}{\lg_k r}+\frac{O(1)}{\lg_k r}.$$

Für $k\geqq 1$ folgt daraus sofort

$$\underline{W}_{i,k}(f)\geqq B. \tag{51}$$

Für $k=0$ ergibt sich $\underline{W}_{i,k}(f)\geqq B\delta$, also mit $\delta\to 1$ ebenfalls (51) und (49).

Es bleibt schließlich noch der Fall $(i,k)=(1,0)$:

Aus (41a) ergibt sich statt (50)

$$|a_n|>\left(\frac{Be}{n}\right)^n,$$

also mit $n=[Br]$

$$M(r)\geqq|a_n|\,r^n>\left(\frac{rBe}{n}\right)^n>e^{Br-1},$$

$$\frac{\lg M(r)}{r}>B-\frac{1}{r},\qquad \underline{W}_{1,0}(f)\geqq B.$$

14. Allgemeiner Wachstumsvergleich

Wir wollen die Untersuchungen über das in 11. eingeführte (i,k)-Wachstum mit einer allgemeinen Betrachtung schließen. Unbefriedigend bleibt, daß bei der durch (11) gegebenen Bewertung der ganzen Funktionen nicht allen Funktionen ein endliches positives Maß zukommt (vgl. 22.). Die Zwischenklassen sind im wesentlichen dadurch bestimmt, daß speziell die Iterierten von e^z als Vergleichsfunktionen benutzt werden. Es werden jedoch gar nicht alle Eigenschaften von

$$\exp_i r=M(r,\exp_i z)$$

gebraucht.

Legt man allgemeiner eine ganze Funktion f als Vergleichsfunktion zugrunde, dann ist zu ersetzen:

$$e^r \quad \text{durch} \quad V(r) = M(r, f),$$

$$\lg x \quad \text{durch} \quad \Lambda(x) = V_{-1}(x) \quad \text{(Umkehrfunktion)}$$

und

$$\overline{\lim_{r\to\infty}}\left(\frac{\lg_{k+i} M(r,g)}{\lg_k r}\right) \quad \text{durch} \quad \overline{\lim_{r\to\infty}}\left(\frac{\Lambda_{k+i} M(r,g)}{\Lambda_k r}\right).$$

(g sei darin eine Funktion, deren Wachstum relativ zu f gemessen werden soll). Sinnvollerweise müßte man fordern, daß $\Lambda(r)$ die Eigenschaften (8)–(10) hat.

Wählt man z.B. $f(z) = \exp(z^m)$ $(m \geqq 2)$, also

$$V(r) = \exp(r^m), \qquad \Lambda(r) = \sqrt[m]{\lg r},$$

dann tritt eine Verjüngung des Maßstabes ein:

Man betrachte etwa die Funktion

$$g(z) = \exp(z^{2m}):$$

Es ist

$$M(r,g) = \exp(r^{2m}), \qquad \Lambda M(r,g) = r^2, \qquad \frac{\Lambda_2 M(r,g)}{\Lambda(r)} = \sqrt[m]{2},$$

während andererseits

$$\varrho(g) = 2m = 2\varrho(f).$$

Betrachtet man den Normaltyp der Ordnung m aus dieser Sicht, dann ergibt sich im Gegensatz zur üblichen Definition

$$\overline{\lim_{r\to\infty}}\left(\frac{\lg M(r)}{r^m}\right) = C \tag{52}$$

hier

$$\overline{\lim_{r\to\infty}}\left(\frac{\Lambda M(r)}{r}\right) = \overline{\lim_{r\to\infty}}\left(\frac{\sqrt[m]{\lg M(r)}}{r}\right) = \sqrt[m]{C}. \tag{53}$$

So hätte die Funktion $g(z) = \exp[(az)^m]$ nach (53) das Maß $|a|$, ist jedoch nach (52) vom Normaltyp $|a|^m$. Im Hinblick auf die Zusammensetzung (vgl. Multiplikationssatz) erscheint (53) als die natürliche, sachgemäße Bewertung.

Für Polynome erhält man hier

$$\lim_{r\to\infty}\left(\frac{\sqrt[m]{\lg M(r)}}{\sqrt[m]{\lg r}}\right) = \sqrt[m]{n}.$$

Wählt man also eine Vergleichsfunktion von unendlicher Ordnung, dann haben die Polynome sämtlich das Maß 1.

Das (i,k)-Wachstum nimmt also eine Sonderstellung ein: Es mißt gerade den Grad der Polynome — und, was besonders wichtig ist, es enthält den Ordnungsbegriff als Spezialfall.

Die Koeffizientenformel (40a) bietet eine weitere Möglichkeit zu einem verallgemeinerten Wachstumsvergleich. Wir wollen hier abschließend nur noch auf folgende bemerkenswerte Analogie hinweisen:

Setzt man in (40a) $k=0$ und $b_n=1$ (für alle n), dann erhält man einen Vergleich mit der Potenzreihe von

$$f(z)=\frac{1}{1-z}, \tag{54}$$

die den Konvergenzradius 1 hat, und (40a) geht in die Koeffizientenformel für den Konvergenzradius über:

$$\overline{\lim_{n\to\infty}}\sqrt[n]{|a_n|}=\frac{1}{R}.$$

Potenzreihen mit großem Konvergenzradius haben also relativ zu (54) kleines Wachstum, die ganzen Funktionen das Wachstum 0.

2. Das Wachstum zusammengesetzter Funktionen

21. Multiplikationssatz

Zum Beweise des Multiplikationssatzes verwenden wir einen Satz von Pólya [29], der zunächst in etwas abgewandelter Form gezeigt werden soll:

Satz 5. *f und g seien ganze (nicht konstante) Funktionen; dann gilt für $r\geqq r_0(g)$*

$$M\Big(M\Big(\frac{r}{6},g\Big),f\Big)\leqq M\big(r,f(g)\big)\leqq M\big(M(r,g),f\big). \tag{55}$$

Die zweite Ungleichung ist ohne weiteres klar. Zum Beweise der ersten benutzen wir folgenden Satz von Bohr [30]:

$w=h(z)$ sei eine in $|z|\leqq 1$ reguläre Funktion mit $h(0)=0$ und $M(\varrho,h)=1$ $(0<\varrho<1)$. $R(h,\varrho)$ bezeichne den Radius des größten Kreises um $w=0$, dessen Peripherie noch ganz im Bild von $|z|\leqq 1$ liegt, also

$$\{z\,|\,|z|\leqq 1\}\xrightarrow{h}\mathfrak{M}_1>\{w\,|\,|w|=R(h,\varrho)\}.$$

Dann hat $R(h,\varrho)$ eine von h unabhängige Mindestgröße:

$$R(h,\varrho)\geqq C(\varrho)>0.$$

Hayman [31] zeigt, daß

$$C(\varrho)=\frac{(1-\varrho)^2}{4\varrho}. \tag{56}$$

Für eine ganze Funktion h^* mit $h^*(0)=0$ und $0<r'<r$ erfüllt die Hilfsfunktion

$$h(z)=\frac{h^*(rz)}{M(r',h^*)}\qquad\Big(\varrho=\frac{r'}{r}\Big)$$

obige Voraussetzungen, also

$$\{z\,||z|\leqq r\}\xrightarrow{h^*}\mathfrak{M}_2>\{w\,||w|=R(r',r,h^*)\},$$

wobei

$$R(r', r, h^*) \geqq C(\varrho)\, M(r', h^*). \tag{57}$$

Ist schließlich $g(z)$ eine beliebige ganze Funktion, dann folgt mit $h^* = g - g(0)$

$$\{z \,|\, |z| \leqq r\} \xrightarrow{g} \mathfrak{M}_3 \supset \{w \,|\, |w - g(0)| = R(r', r, g - g(0))\}$$

und aus (57)

$$R(r', r, g - g(0)) \geqq C(\varrho)\, M(r', g - g(0)) \geqq C(\varrho)\, (M(r', g) - |g(0)|).$$

Nunmehr läßt sich abschätzen:

$$M(r, f(g)) \geqq M(r_1, f), \tag{58}$$

worin $r_1 = C M(r', g) - (C+1)\,|g(0)|$ (ϱ fest; r' so groß, daß $r_1 > 0$). Wählt man speziell $r' = \frac{r}{6}$, dann wird nach (56) $C > 1$, also für $r \geqq r_0(g)$

$$r_1 \geqq M\left(\frac{r}{6}, g\right),$$

und in Verbindung mit (58) folgt (55).

In leichter Abwandlung brauchen wir außerdem

$$M(r, f(g)) \geqq M\left(\frac{C}{2} M(\varrho r, g), f\right), \quad (r \geqq r_0(g)). \tag{59}$$

Jetzt läßt sich der wesentliche Zusammenhang zwischen Zusammensetzung und Wachstum beschreiben:

Es sei wieder $h = f(g)$. Dann folgt aus Satz 5 für $r \geqq r_0(g)$

$$\frac{\lg_{k+i} M(r, h)}{\lg_k r} \leqq \frac{\lg_{k+i} M(M(r, g), f)}{\lg_{k+i_2} M(r, g)} \cdot \frac{\lg_{k+i_2} M(r, g)}{\lg_k r}, \tag{60}$$

wobei $0 \leqq i_2 \leqq i$, und für $k \geqq 1$

$$\frac{\lg_{k+i} M(r, h)}{\lg_k r} \geqq \frac{\lg_{k+i} M\left(M\left(\frac{r}{6}, g\right), f\right)}{\lg_{k+i_2} M\left(\frac{r}{6}, g\right)} \cdot \frac{\lg_{k+i_2} M\left(\frac{r}{6}, g\right)}{\lg_k \frac{r}{6} + \lg 6}. \tag{61a}$$

Für $k = 0$ und $i_2 \geqq 1$ sei in (59) $\frac{C}{2} < 1$ (also etwa $\frac{1}{2} < \varrho < 1$). Dann folgt für $r \geqq r_0(g)$

$$\frac{\lg_i M(r, h)}{r} \geqq \frac{\lg_i M\left(\frac{C}{2} M(\varrho r, g), f\right)}{\lg_{i_2}\left(\frac{C}{2} \cdot M(\varrho r, g)\right)} \cdot \frac{\lg_{i_2} M(\varrho r, g) - \lg \frac{2}{C}}{\varrho r} \cdot \varrho. \tag{61b}$$

In abgekürzter Schreibweise sei (mit $i_1 + i_2 = i$, $i_{1,2} \geqq 0$)

$$W_{i,k}(h) = H, \quad W_{i_1, k+i_2}(f) = F, \quad W_{i_2, k}(g) = G,$$

und analog $\underline{W}_{i,k}(h) = \underline{H}$, usw. Es folgt

SATZ 6 (Multiplikationssatz):

$$\text{(62a)} \qquad \begin{cases} \overline{F\,\overline{G}} \geqq \overline{H} \geqq \overline{F}\,\underline{G} \geqq \underline{H} \geqq \underline{F}\,\underline{G}, \\ \overline{H} \geqq \underline{F}\,\overline{G} \geqq \underline{H}. \end{cases}$$

Falls oberes und unteres Wachstum bei einer Funktion zusammenfallen,

$$\text{(62b)} \qquad \begin{cases} \overline{H} = F\overline{G}, & \overline{H} = \overline{F}\,G, \\ \underline{H} = F\underline{G}, & \underline{H} = \underline{F}\,G, \end{cases} \qquad H = \overline{F}\,\underline{G} = \underline{F}\,\overline{G},$$

falls bei zwei Funktionen, dann allgemein

$$\text{(62c)} \qquad H = FG.$$

(Wir treffen hierbei die Vereinbarung, daß $a \cdot \infty = \infty$ für $a > 0$, im Falle $0 \cdot \infty$ aber die Formeln (62) ohne jede Aussage sind.)

Für $k \geqq 1$ folgt (62) durch den Grenzübergang $r \to \infty$ in (60) und (61a). Bei $k = 0$, $i_2 = 0$ ist entweder $W_{0,0}(g) = \infty$ und der Faktor $\frac{1}{6}$ stört nicht, oder $g(z) = az + b$. Dann aber gilt Satz 5 schärfer, d.h. für $r \geqq r_0(\varepsilon)$ kann in (55) statt $\frac{1}{6}$ der Faktor $(1-\varepsilon)$ gesetzt werden. Falls $k = 0$, $i_2 \geqq 1$, dann mache man den Grenzübergang $r \to \infty$ in (61b) für jedes feste $\varrho < 1$. Somit ist Satz 6 vollständig bewiesen. – (Der Multiplikationssatz stimmt auch, falls f oder g konstant ist, weil dann trivialerweise stets $FG = H = 0$.)

Eine scharfe Aussage geben (62b) und (62c). Deshalb ist es wichtig zu wissen, wann oberes und unteres Wachstum übereinstimmen. Das ist bei vielen bekannten Funktionen der Fall, so daß sich bei speziellen Fragen der Multiplikationssatz meist in seiner scharfen Form anwenden läßt. Da stets $\underline{W}_{0,0} = \overline{W}_{0,0}$ und $\underline{W}_{0,1} = \overline{W}_{0,1}$, beschreibt (62c) z.B. auch die Gesetzmäßigkeiten bei der Zusammensetzung von linearen Funktionen und Polynomen.

Wir können nun auch in Ergänzung von Abschnitt 1. zeigen, *daß das (i, k)-Wachstum gegenüber Translationen invariant ist:*

Mit $g = z + a$, also $W_{0,0}(g) = 1$, folgt gemäß (62b)

$$\overline{W}_{i,k}\big(f(z+a)\big) = \overline{W}_{i,k}(f) \cdot 1,$$
$$\underline{W}_{i,k}\big(f(z+a)\big) = \underline{W}_{i,k}(f) \cdot 1.$$

Damit gilt insbesondere Satz 4 für Potenzreihenentwicklungen

$$f(z) = \sum a_n (z - z_0)^n$$

bei beliebigem z_0.

Aber auch die Ungleichungen (62a) lassen sofort eine interessante Folgerung zu. Wir fragen nach Teilmengen der ganzen Funktionen, die bezüglich der Zusammensetzung abgeschlossen sind. Wegen des algebraischen Charakters der Zusammensetzung erzeugt natürlich jede beliebige Basis eine solche abgeschlossene Hülle (eine einzelne Funktion $f(z)$ z.B. die Menge ihrer Iterierten $f_n(z)$, $n = 1, 2, \ldots$). Demgegenüber gibt es aber auch abgeschlossene Teilmengen mehr analytischen Charakters, z.B. die linearen Funktionen, die Polynome. Allgemeiner gilt

SATZ 7. *Die* $H_{0,k}$ $(k=0, 1, \ldots)$ (vgl. Def. (12a)) *sind einzeln bezüglich der Zusammensetzung abgeschlossen.*

Innerhalb der Ordnung 0, gewissermaßen „an ihrem unteren Rande", gibt es also abzählbar viele Wachstumsgrenzen, die bei Zusammensetzung nicht übersprungen werden. $k=0, 1$ liefert die oben genannten Spezialfälle, ab $k=2$ sind aber auch transzendente Funktionen einbegriffen.

Der Beweis folgt unmittelbar aus (62a):

$$\overline{W}_{0,k}(f(g)) \leqq \overline{W}_{0,k}(f) \cdot \overline{W}_{0,k}(g),$$

haben also f und g endliches $(0, k)$-Wachstum, dann auch $f(g)$. (Man beachte, daß für $k \geqq 1$ stets $\underline{W}_{0,k} \geqq 1$ ist.)

Es gibt natürlich außer den in Satz 7 genannten Wachstumsgrenzen noch weitere, z. B. sind auch die Mengen aller Funktionen mit $\overline{W}_{0,k}=1$, die allgemein nicht etwa mit $H_{0,k-1}$ identisch sind (vgl. 22.), wachstumsabgeschlossen.

22. Beispiele

Jetzt lassen sich auch die in der Einleitung zitierten Beispiele (7) von BAKER diskutieren. Am einfachsten ist die Behandlung von

$$f_3(z) = \sum \exp[-n(\lg n)^2]\, z^n:$$

Wir berechnen nach Satz 4

$$W_{1,2}(f_3) = \lim_{n\to\infty}\left(\frac{\lg\lg n}{\lg(\lg n)^2}\right) = \frac{1}{2}.$$

Es ist also $f_3 \in H_{1,2}$, $W_{1,3}(f_3)=1$ und, wie behauptet, $W_{1,1}(f_3)=\varrho(f_3)=0$. Nach dem Multiplikationssatz folgt weiter

$$W_{2,2}(f_3(f_3)) = W_{1,3}(f_3)\cdot W_{1,2}(f_3) = \tfrac{1}{2},$$

d. h. $f_3(f_3) \in H_{2,2}$ und damit natürlich von unendlicher Ordnung. Das erste Beispiel (7a) lautet

$$f_1(z) = \sum \exp(-n^2)\, z^n.$$

Man kann abschätzen:

$$M(r) = \sum_{n=0}^{\infty}\left(\frac{r}{e^n}\right)^n = \sum_{n=0}^{n_1} + \sum_{n=n_1+1}^{\infty}.$$

$n_1 = \lceil \lg 2r \rceil$ $(r \geqq 1)$ ergibt $\Sigma_2 \leqq 1$ und

$$\Sigma_1 \leqq (n_1+1)\, r^{n_1} \leqq (\lg 2r + 1)\, e^{\lg r \cdot \lg 2r};$$

daraus folgt

$$\overline{W}_{0,2}(f_1) = \overline{\lim_{r\to\infty}}\left(\frac{\lg\lg M(r)}{\lg\lg r}\right) \leqq 2.$$

f_1 ist also aus $H_{0,2}$ und $\varrho(f_1)=0$. Nach Satz 7 trifft das dann aber auch für alle Iterierten von f_1 zu.

Das Beispiel (7b) schließlich wollen wir etwas abwandeln, um es den hier verwandten Methoden anzupassen.

BAKER konstruiert eine reelle Funktion $p(x)$, die für $x \geqq 0$ $p(p(x)) = e^x$ erfüllt; sie ist monoton wachsend, konvex nach unten und genügt (vgl. (8))

$$\lim_{x\to\infty}\left(\frac{x}{p(x)}\right) = 0.$$

$p_{-1}(x)$ ist also ein Halblogarithmus, und die geradzahligen Iterierten dieser Funktion sind die Iterierten von $\lg x$. Wir untersuchen

$$f_2(z) = \sum_{n=1}^{\infty} \frac{z^n}{[p(n)]^n}; \tag{63}$$

$$W_{1,k}(f_2) = \lim_{n\to\infty}\left(\frac{\lg_k n}{\lg_k p(n)}\right) = \lim_{n\to\infty}\left(\frac{\lg_k n}{p(\lg_k n)}\right) = 0 \quad \text{für alle } k \geqq 1,$$

also $f_2 \notin H_1$ und $\varrho(f_2) = 0$.

Andererseits ist

$$M(r) > \left(\frac{r}{p(n)}\right)^n,$$

$$\lg M(r) > n\left(\lg r - p_{-1}(n)\right).$$

Wir wählen $n = \left[p_{-1}\left(\frac{r}{e}\right)\right]$ und erhalten

$$\lg M(r) > p_{-1}\left(\frac{r}{e}\right) - 1,$$

$$\lim_{r\to\infty}\left(\frac{\lg_k M(r)}{\lg_k r}\right) \geqq \lim_{r\to\infty}\left(\frac{p\left(\lg_k \frac{r}{e}\right)}{\lg_k r}\right) = \infty.$$

Damit ist auch $f_2 \notin H_0$, also $f_2 \in Z_0$ gezeigt.

In Weiterbehandlung des Beispiels ergibt sich

$$\lim_{r\to\infty}\left(\frac{p_{-1}(\lg M(r))}{\lg r}\right) = 1.$$

f_2 hätte also, in analoger Verallgemeinerung von (11), das Wachstum $W_{\frac{1}{2},1}(f_2) = 1$ und $W_{\frac{1}{2},\frac{1}{2}}(f_2) = 1$. Wendet man nun den Multiplikationssatz an (der sich mittels der Eigenschaften von $p(x)$ auch auf diesen Fall übertragen läßt), dann folgt

$$W_{1,1}(f_2(f_2)) = W_{\frac{1}{2},\frac{1}{2}}(f_2)\, W_{\frac{1}{2},1}(f_2) = 1.$$

Man sieht, daß sich auf dem gleichen Wege zu beliebigem m Funktionen $g(z)$ konstruieren lassen, so daß $g_m(z)$ von endlicher positiver Ordnung ist. Es liegt überhaupt nahe, mittels einer kontinuierlichen Schar reeller Iterierter von $\lg x$ das (i, k)-Wachstum allgemein für reelle Paare (i, k) zu definieren. BÖDEWADT [17] gibt eine Konstruktion für $\exp_a x$ (a beliebig reell). Bei der Behandlung spezieller Fragen dürften sich auf jenem Wege jedoch große Schwierigkeiten ergeben, da man zu wenig über diese Iterierten weiß.

Für die Iterierten von e^z ergibt der Multiplikationssatz durch wiederholte Anwendung

$$W_{i,k}(\exp_i z) = 1 \qquad (i, k \geqq 0).$$

Allgemeiner läßt sich folgern:

SATZ 8. *f, g, h seien von regulärem Wachstum:*
Aus $f \in H_i$, $g \in H_j$ folgt dann $f(g) \in H_{i+j}$, aus $h \in H_i$ also $h_m(z) \in H_{m+i}$.

Das (i, k)-Wachstum beschreibt also im wesentlichen das Wachstum von Funktionen f, die mit einer Iterierten der Exponentialfunktion wachstumsverwandt sind (in dem Sinne, daß $f \in H_i$), und ihrer Zusammensetzungen. Daß damit jedoch nicht alle ganzen Funktionen erfaßt sind, wollen wir nunmehr zeigen.

Das Beispiel (63) ermöglicht sofort den Nachweis, daß die Z_i nicht leer sind, denn nach dem Multiplikationssatz folgt z. B.

$$\exp_i(f_2) \in Z_i, \qquad f_2(\exp_i z) \in Z_i.$$

Weiter geben wir zwei Funktionen aus Z_∞ an:

Zunächst konstruieren wir eine Hilfsfolge ganzer Zahlen

$$t_n = \max\{t \mid \exp_{2t} 1 \leqq n\} \qquad (n \geqq 1),$$

für die offensichtlich $t_n \to \infty$ gilt, und betrachten

$$h(z) = \sum_{n=1}^{\infty} (\lg_{t_n} n)^{-n} z^n:$$

$h(z)$ ist eine ganze Funktion, denn

$$\sqrt[n]{\frac{1}{|a_n|}} = \lg_{t_n} n \geqq \exp_{t_n} 1 \to \infty.$$

Andererseits ist nach Satz 4 (für $i \geqq 2$)

$$W_{i,0}(h) = \lim_{n \to \infty} \left(\frac{\lg_{i-1} n}{\lg_{t_n} n} \right) = \infty$$

und damit nach Definition (12d) $h \in Z_\infty$.

Das zweite Beispiel ist der Iterationstheorie entnommen: $S(z)$ sei die Schrödersche Funktion zu einem der (abstoßenden) Fixpunkte von e^z (vgl. TÖPFER [14] und KNESER [28]). Dann gilt in einer Umgebung von $a = e^a$ ($|a| > 1$)

$$S(e^z) = a\, S(z).$$

Mit $z = S_{-1}(w)$ folgt für eine Umgebung von $w = 0$

$$\exp[S_{-1}(w)] = S_{-1}(a\, w). \tag{64}$$

Wegen $|a| > 1$ läßt sich $S_{-1}(w)$ mittels (64) eindeutig in die ganze w-Ebene fortsetzen, ist also eine ganze Funktion.

Auf (64) wenden wir den Multiplikationssatz an:

$$\underline{W}_{i+1,0}(\exp S_{-1}) = W_{1,i}(e^1)\,\underline{W}_{i,0}(S_{-1}) = \underline{W}_{i,0}(S_{-1}),$$

andererseits aber

$$\underline{W}_{i+1,0}\big(S_{-1}(aw)\big) = \underline{W}_{i+1,0}(S_{-1})\cdot|a|,$$

also

$$\underline{W}_{i+1,0}(S_{-1}) = \frac{1}{|a|}\cdot\underline{W}_{i,0}(S_{-1}).$$

Wegen $W_{0,0}(S_{-1}) = \infty$ folgt daraus $W_{i,0}(S_{-1}) = \infty$ für alle i und damit $S_{-1}\in Z_\infty$.

Im Gegensatz zu den vorangehenden Beispielen geben wir schließlich noch eine transzendente Funktion von sehr geringem Wachstum an, mit der wir gleichzeitig nachweisen wollen, daß aus $W_{0,k+1}(g) = 1$ allgemein nicht $g\in H_{0,k}$ folgt, daß also unsere Wachstumsskala selbst innerhalb H_0 noch nicht so fein unterscheidet, daß es zu jedem transzendenten $f\in H_0$ ein k mit $1 < \overline{W}_{0,k}(f) < \infty$ gibt:

$$g(z) = \sum_{n=0}^{\infty} (\exp_2 n)^{-n} z^n:$$

Wie an früherer Stelle schätzt man mit $n_1 = [\lg_2 2r]$ ab:

$$M(r) = \Sigma(\exp_2 n)^{-n} r^n = \Sigma_1 + \Sigma_2,$$

$$\Sigma_2 \leqq 1, \qquad \Sigma_1 \leqq (\lg_2 2r + 1)\, r^{\lg_2 2r},$$

$$\lg M(r) \leqq \lg_3 2r + 2 + \lg_2 2r \cdot \lg r,$$

$$\frac{\lg\lg M(r)}{\lg\lg r} \leqq \frac{\lg_4 2r + 2 + \lg_3 2r}{\lg_2 r} + 1.$$

Der Grenzübergang ergibt $W_{0,2}(g) = 1$, während andererseits für eine transzendente Funktion aber stets $W_{0,1}(g) = \infty$.

23. Verallgemeinerung eines Satzes von PÓLYA

Der Vollständigkeit halber wollen wir folgenden Satz von PÓLYA [29] auf die höheren Wachstumsstufen ausdehnen:

SATZ von PÓLYA. *Es sei* $\varrho\big(f(g)\big) = C < \infty$. *Dann ist entweder* g *ein Polynom* n*-ten Grades und* $\varrho(f) \leqq \frac{C}{n}$ *oder* $\varrho(f) = 0$ *und* $\varrho(g) \leqq C$.

Wir zeigen in Analogie

SATZ 9. *Es sei* $\overline{W}_{i,1}\big(f(g)\big) = C < \infty$ $(i \geqq 1)$. *Dann ist entweder* g *ein Polynom* n*-ten Grades und* $\overline{W}_{i,1}(f) = \frac{C}{n}$ *oder* $W_{i,1}(f) = 0$ *und* $\overline{W}_{i,1}(g) \leqq C$.

Der Beweis folgt direkt aus dem Multiplikationssatz:

$$\overline{W}_{i,1}\big(f(g)\big) = \overline{W}_{i,1}(f)\cdot W_{0,1}(g).$$

Ist g ein Polynom, dann folgt unmittelbar obige Behauptung. Ist g aber transzendent, also $W_{0,1}(g) = \infty$, dann würde aus $\overline{W}_{i,1}(f) > 0 \quad C = \infty$ folgen.

Die letzte Ungleichung von Satz 9 besteht für nicht lineare Funktionen allgemein, d. h. *die Komponenten haben höchstens das Wachstum der zusammengesetzten Funktion*. Denn nach (62a) folgt

$$\overline{W}_{i,k}(f(g)) \geqq \underline{W}_{0,k+i}(f) \cdot \overline{W}_{i,k}(g),$$
$$\underline{W}_{i,k}(f(g)) \geqq \underline{W}_{0,k+i}(f) \cdot \underline{W}_{i,k}(g),$$

und es ist (f und g sollen nicht linear sein) $\underline{W}_{0,k+i}(f) \geqq 1$. Für f schließt man umgekehrt genau so.

24. Anwendungen auf die Funktionalgleichung $f(f(z)) = F(z)$ und verwandte Fragen

In diesem Abschnitt soll schließlich an zwei Beispielen gezeigt werden, wie die vorangehenden Wachstumsbetrachtungen auf Fragen der Zerlegbarkeit von ganzen Funktionen angewandt werden können. Bekannt sind hier z. B. schon folgende Ergebnisse:

a) Wenn g transzendent und von endlicher Ordnung ist und einen Wert nur endlich oft annimmt, dann hat $f(f(z)) = g(z)$ keine ganze Lösung f (BAKER [24], THRON [23]).

b) e^z ist nur mit den Iterierten $\exp_i z$ vertauschbar (BAKER [25]).

(f und g heißen vertauschbar, wenn $f(g) = g(f)$.)

Wir betrachten Funktionen unendlicher Ordnung, genauer aus H_2, und zeigen

SATZ 10. *$f(z)$ sei ganz. Aus $f(f(z)) \neq a$ und $\overline{W}_{2,1}(f(f)) = C < \infty$ folgt dann $f(z) = a + \exp(P_n(z))$ und $n = C$.*

Wegen $f(f) \neq a$ ist $f(f) = a + e^h$ (h ganz). Nach dem Picardschen Satz hat auch f den vollständigen Ausnahmewert a, also $f = a + e^g$, $f(f) = a + \exp[g(a + e^g)]$ und

$$h = g(a + e^g) + 2m\pi i. \tag{65}$$

Der Multiplikationssatz ergibt

$$\begin{cases} C = \overline{W}_{2,1}(f(f)) = \overline{W}_{2,1}(e^h) = \overline{W}_{1,1}(h), \\ W_{1,1}(a + e^g) = W_{1,1}(e^g) = W_{0,1}(g). \end{cases} \tag{66}$$

(65) und (66) liefern

$$C = \overline{W}_{1,1}(g(a + e^g)) = \overline{W}_{0,2}(g) \cdot W_{0,1}(g).$$

Wegen $C < \infty$ und $\overline{W}_{0,2}(g) \geqq 1$ ist $W_{0,1}(g) < \infty$, also $g = P_n(z)$, $W_{0,1}(g) = n$, $W_{0,2}(g) = 1$ und $C = n$.

Speziell folgt nun aus Satz 10, daß die Funktionalgleichung

$$f(f(z)) = F(z), \tag{67}$$

z. B. für $F = e^{\sin z}$, $F = \exp\left(\frac{1}{\Gamma(z)}\right)$ oder ähnliche Funktionen, insbesondere auch für $F(z) = \exp_2(az)$ ($a \neq 0, 1$), keine ganze Lösung besitzt. Ein allgemeineres notwendiges Kriterium für die Existenz einer ganzen Lösung von

(67) ist (unter den Voraussetzungen von Satz 10), daß F von regulärem $(2, 1)$-Wachstum und $W_{2,1}(F)$ eine ganze Zahl ist.

Eine Aussage über die Vertauschbarkeit von ganzen Funktionen gibt

SATZ 11. *Ist $f \in H_i$ von regulärem Wachstum, $g \in H_j$ $(i, j \geqq 1)$ und $f(g) = g(f)$, dann gilt für alle $k \geqq 0$ $W_{i,k}(f) = \overline{W}_{j,k}(g)$.*

BEWEIS:

$$(68). \qquad \begin{cases} \overline{W}_{i+j,k}(f(g)) = W_{i,k+j}(f) \cdot \overline{W}_{j,k}(g), \\ \overline{W}_{i+j,k}(g(f)) = \overline{W}_{j,k+i}(g) \cdot W_{i,k}(f). \end{cases}$$

Wegen $f \in H_i$, $g \in H_j$ gibt es ein minimales k' mit $0 < W_{i,k'}(f) < \infty$ und $0 < \overline{W}_{j,k'}(g) < \infty$, also wegen $i, j \geqq 1$ $W_{i,k'+j}(f) = 1$, $\overline{W}_{j,k'+i}(g) = 1$.

Setzt man in (68) $k = k'$, dann folgt die Behauptung für k', damit wegen (8c) aber auch für alle $k > k'$. Ist nun $k' > 0$, dann folgt aus (68) für $k = k' - 1$, weil k' minimal gewählt wurde, entweder $W_{i,k}(f) = \overline{W}_{j,k}(g) = 0$ oder $W_{i,k}(f) = \overline{W}_{j,k}(g) = \infty$, womit die Behauptung auch für alle $k < k'$ bewiesen ist.

Satz 11 läßt eine Reihe von Folgerungen zu. Zwei Funktionen endlicher positiver Ordnung (eine von ihnen sei von regulärem Wachstum) können nur vertauschbar sein, wenn sie von gleicher Ordnung sind. Spezieller kann z. B. $\sin z$ als Funktion vom Normaltyp 1 der Ordnung 1 mit einer Funktion g von positiver endlicher Ordnung nur vertauschbar sein, wenn g ebenfalls vom Normaltyp 1 der Ordnung 1 ist.

Allgemeiner werden sich die von Satz 10 und Satz 11 berührten Fragen jedoch erst behandeln lassen, wenn man neben dem Wachstum auch die Werteverteilung zusammengesetzter Funktionen näher untersucht.

Literatur

[1] SCHRÖDER, E.: Über unendlich viele Algorithmen zur Auflösung der Gleichungen. Math. Ann. **2**, 317–365 (1870). — [2] SCHRÖDER, E.: Über iterierte Funktionen. Math. Ann. **3**, 296–322 (1871). — [3] KOENIGS, G.: Recherches sur les équations fonctionelles. Ann. de l'École norm. III, 1 (1884), Suppl. — [4] JULIA, G.: Mémoire sur l'itération de fonctions rationelles. J. Math. **8**, 1 (1918). — [5] FATOU, P.: Sur les équations fonctionelles. Bull. Soc. Math. France **47**, 161–271 (1919); **48**, 33–94, 208–314 (1920). — [6] FATOU, P.: Sur l'itération des fonctions transcendantes entières. Acta Math. **47**, 337–370 (1926). — [7] RITT, J. F.: On the iteration of rational functions. Trans Amer. Math. Soc. **21**, 348–356 (1920). — [8] HADAMARD, J.: Two works on iteration and related questions. Bull. Amer. Math. Soc. **50**, 67–75 (1944). — [9] CREMER, H.: Über die Iteration rationaler Funktionen. Jahresb. dtsch. Math.-Ver. **33** (1925). — [10] CREMER, H.: Zum Zentrumproblem. Math. Ann. **98** (1927). — [11] CREMER, H.: Über die Häufigkeit der Nichtzentren. Math. Ann. **115**, 573–580 (1938). — [12] SIEGEL, C. L.: Iteration of analytic functions. Ann. Math. **43**, 607–612 (1942). — [13] TÖPFER, H.: Über die Iteration der ganzen transzendenten Funktionen, insbesondere von $\sin z$ und $\cos z$. Math. Ann. **117**, 65–84 (1939). — [14] TÖPFER, H.: Komplexe Iterationsindizes. Math. Ann. **121**, 191–222 (1949). — [15] CREMER, H.: Über das Zentrumproblem. Sächs. Akademieber. **82** (1930). — [16] CREMER, H.: Über die Schrödersche Funktionalgleichung und das Schwarzsche Eckenabbildungsproblem. Sächs. Akademieber. **84** (1933). — [17] BÖDEWADT, U. T.: Zur Iteration reeller Funktionen. Math. Z. **49**, 497–516 (1943). — [18] ISAACS, R.: Iterates of fractional order. Can. J. Math. **2**, 409–416 (1950). — [19] MONTEL, P.: Leçons sur les récurrences et leurs applications. Paris: Gauthier-Villars 1957. — [20] RITT, J. F.:

Prime and composite polynomials. Trans. Amer. Math. Soc. **23**, 51–66 (1922). – [21] JACOBSTHAL, E.: Über vertauschbare Polynome. Math. Z. **63**, 243–276 (1955). – [22] ROSENBLOOM, P. C.: The fix-points of entire functions. Medd. Lunds Univ. Math. Sem., Suppl.-Bd. 186–192 (1952). – [23] THRON, W. J.: Entire solutions of the functional equation $f(f(z)) = g(z)$. Can. J. Math. **8**, 47–48 (1956). – [24] BAKER, I. N.: The iteration of entire transcendental functions and the solution of the functional equation $f(f(z)) = F(z)$. Math. Ann. **129**, 174–180 (1955). – [25] BAKER, I. N.: Zusammensetzungen ganzer Funktionen. Math. Z. **69**, 121–163 (1958). – [26] OSSERMANN, R.: On the solution of $f(f(z)) = e^z - 1$ and its domains of regularity. Proc. Amer. Math. Soc. **8**, 262–263 (1957). – [27] CRUM, M.: On two functional equations, which occur in the theory of clockgraduation. Quart. J. Math. Oxford Ser. **10**, 155–160 (1939). – [28] KNESER, H.: Reelle analytische Lösungen der Gleichung $f(f(x)) = e^x$ und verwandte Funktionalgleichungen. J. reine u. angew. Math. **187**, 56–67 (1950). – [29] PÓLYA, G.: On an integral function of an integral function. J. Lond. Math. Soc. **1** 12–15 (1926). – [30] BOHR, H.: Über einen Satz von Edmund Landau. Scripta Univ. Hierosolymitanarum **1**, Nr. 2 (1923). – [31] HAYMAN, W. K.: Symmetrization in the theory of functions. Stanford Univ. Techn. Report, No. 11 (1950). – [32] PRINGSHEIM, A.: Elementare Theorie der Funktionen endlicher Ordnung. Math. Ann. **58**, 257–342 (1904). – [33] NEVANLINNA, R.: Eindeutige analytische Funktionen. Berlin: Springer 1953.

Köln, Institut für angewandte Mathematik der Universität

(Eingegangen am 6. April 1959)

LILLO, J. C.
Math. Zeitschr. 73, 45–58 (1960)

Continuous Matrices and the Stability Theory of Differential Systems

Von

JAMES C. LILLO*)

1. Introduction and Notation

In this paper we shall be primarily interested in systems of the form

$$\dot{x} = [A(t) + B(t)]\, x, \tag{1.1}$$

where $A(t)$ and $B(t)$ are continuous and uniformly bounded for $0 \leqq t < \infty$. In the second section we consider the question of kinematic similarity [5] for systems of the form (1.1). The main results here are found in the Corollaries 2.2 and 2.3. In the third section we consider the stability question for bounded solutions of systems of the form $\dot{x} = \mathfrak{F}(x, \mu, t)$ [Theorem 3.1]. In the fourth section we introduce a more general kind of similarity which we call approximate similarity. We then show that a rather large class of matrices are approximately similar to a constant matrix. In section five we use the results obtained in the earlier sections to study stability theory for non-linear differential systems.

We introduce the following definitions and notation. If the continuous function $a(t)$, $0 \leqq t < \infty$, possesses a mean value λ we write $M[a(t)] = \lambda$. The associated constants $T(\varepsilon)$ and $M(\varepsilon)$ such that

$$\left| \int_{t_0}^{t_0 + T(\varepsilon) + \sigma} [a(t) - \lambda]\, dt \right| \leqq \varepsilon \left(T(\varepsilon) + \sigma \right)$$

for all $\sigma \geqq 0$ and

$$\left| \int_{t_0}^{t_0 + t} [a(s) - \lambda]\, ds \right| < M(\varepsilon) + \varepsilon\, t$$

for all $t \geqq 0$ will be referred to as the constants of the mean with the initial time t_0. A continuous function $a(t)$ is said to possess property A [A*] with mean λ (real) if for every $\mu > 0$ there exists a constant $M(\mu)$ such that

$$\left| \int_s^t [a(\tau) - \lambda]\, d\tau \right| < M(\mu) + \mu\, |t - s| \quad \text{for all} \quad 0 \leqq t, s \leqq \infty \; [-\infty < t, s < \infty].$$

The norm, written $||A(t_k)||$, of a constant $n \times m$ matrix is defined as

$$||A(t_k)|| = \sum_{i,j} |a_{ij}(t_k)|$$

*) This research was sponsored by the Office of Ordnance Research, U.S. Army. Contract Co. DA-23-072-ORD-1289.

and the norm, written $||A||$, of a variable matrix $A(t)$, $t \in R$, is $||A|| = \operatorname{lub}_{t \in R} ||A(t)||$. In sections two, three, and four, R is the half line $0 \leqq t < \infty$. In some of the applications R is the entire real line. We shall denote the j-th column and k-th row of the matrix $A(t)$ by $[A(t)]_j$ and $[A(t)]^k$ respectively.

The solution $x(t)$ of (1.1) is said to have the characteristic exponent λ, written C.E. $[x(t)] = \lambda$, if $\overline{\lim_{t \to \infty}} [\ln ||x(t)||/t] = \lambda$ and is said to possess the strong charcteristic exponent λ, written S.C.E. $[x(t)] = \lambda$, if $\lim_{t \to \infty} [\ln ||x(t)||/t] = \lambda$. Let $\lambda_1 < \lambda_2 < \cdots < \lambda_k$ be the set of all distinct values assumed by C.E. $[x(t)]$ where $x(t)$ is any solution of (1.1). Let e_1 be the number of linearly independent solutions $x(t)$ for which C.E. $[x(t)] = \lambda_1$ and let $\sum_{i=1}^{s} e_i$ be the number of linearly independent solutions $x(t)$ for which C.E. $[x(t)] = \lambda_s$. The e_i is called the multiplicity of λ_i and the system is said to possess the characteristic exponents $\lambda_1, \ldots, \lambda_n$, written C.E. $[\lambda_1, \ldots, \lambda_n]$, where exponents of multiplicity j are written j times. In the case in which all the solutions of system (1.1) possess strong characteristic exponents we may, as above, let $\lambda_1 < \lambda_2 < \cdots < \lambda_k$ be the set of all distinct values assumed by S.C.E. $[x(t)]$ where $x(t)$ is any solution of (1.1). Let e_1 be the number of linearly independent solutions $x(t)$ for which S.C.E. $[x(t)] = \lambda_1$ and let $\sum_{i=1}^{s} e_i$ be the number of linearly independent solutions $x(t)$ for which S.E.C. $[x(t)] = \lambda_s$. Then e_i is called the multiplicity of λ_i and the system is said to possess the strong characteristic exponents $\lambda_1, \ldots, \lambda_n$, written S.C.E. $[\lambda_1, \ldots, \lambda_n]$ where exponents of multiplicity j are written j times. For any linear system of the form $\dot{x} = A(t)\,x$ the natural base for $t = t_0$ is the fundamental solution $X(t)$ such that $X(t_0) = I$. We denote the natural base for $t = t_0$ by $X(t, t_0)$ and its columns by $[X(t, t_0)]_i$ where

$$[X(t_0, t_0)]_i = \operatorname{col}(\delta_{i1}, \ldots, \delta_{in}).$$

The j-th component of $[X(t, t_0)]_i$ is denoted by $[X_j(t, t_0)]_i$. Finally we define M_n to be the set of all continuous $n \times n$ matrices $A(t)$ whose norm $||A||$ is finite, where R is the half line $0 \leqq t < \infty$. The subset of M_n which consists of all upper triangular [diagonal] matrices will be denoted by TM_n [DM_n].

2. Kinematic Similarity

The work of PERRON [6], DILIBERTO [2], and MARKUS [5] assures us that the problem of studying the characteristic exponents for a system of the form

$$\dot{y} = B(t)\,y, \tag{2.1}$$

where $B(t) \in M_n$, is equivalent to the same problem for systems of the form

$$\dot{x} = A(t)\,x, \tag{2.2}$$

where $A(t) \in TM_n$. We shall later see that the diagonal elements of $A(t)$ play a dominant role. For this reason we now establish necessary and sufficient conditions in order that these diagonal terms possess distinct mean values

$\lambda_1, \ldots, \lambda_n$ where $\lambda_i < \lambda_{i+1}$. In preparation for this result we have the following theorems.

THEOREM 2.1. *If for system* (2.2) *the* S.C.E. $[[X(t,0)]_i] = \lambda_i$, $i = 1, \ldots, n$ *and* $\lambda_i < \lambda_{i+1}$ *for* $i = 1, \ldots, n-1$ *then* $M[a_{ii}(t)] = \lambda_i$ *for* $i = 1, \ldots, n$.

Before proceeding to the proof of this theorem we first establish the following three lemmas.

LEMMA 2.1. Suppose $\delta_i = \lambda_n - \lambda_{n-i} > 0$. Then given any positive $\varepsilon_1 < \delta_1/4$, there exists an integer $k > 2$ such that, where

$$\varepsilon_{n-j} = \varepsilon_1/k^{n-j}, \quad j = 0, \ldots, n-2, \quad a_i = (\delta_i + \varepsilon_n)/(\delta_i - \varepsilon_n - \varepsilon_{i+1}),$$
$$b = (M + \varepsilon_1)/(M + \varepsilon_2 + \varepsilon_n), \quad M > 0,$$

one has

$$\prod_{i=1}^{n-1} a_i < b. \tag{2.3}$$

PROOF. Inequality (2.3) may be rewritten in the form

$$\begin{cases} \prod_{i=1}^{n-1} [\delta_i + \varepsilon_1/k^n]\,[M + (\varepsilon_1/k^n)\,(k^{n-2}+1)] \\ \quad < \prod_{i=1}^{n-1} [\delta_i - (\varepsilon_1/k^n)\,(1 + k^{n-(i+1)})]\,[M + \varepsilon_1]. \end{cases} \tag{2.4}$$

However (2.4) is a consequence of

$$\begin{cases} \left[\prod_{i=1}^{n-1} \delta_i + \sum_{j=1}^{n-1} \left((n-1)!/[(n-j)!\,j!]\right)(\varepsilon_1/k^n)^j (\delta_{n-1})^{n-j}\right][M + \varepsilon_1/k^n (k^{n-2}+2)] \\ \quad < \left[\prod_{i=1}^{n-1} \delta_i - \sum_{j=1}^{n-1} \left((n-1)!/[(n-j)!\,j!]\right)\left(\varepsilon_1/k^n [2 + k^{n-2}]\right)^j (\delta_{n-1})^{n-j}\right] \times \\ \quad \times [M + (\varepsilon_1/k^n)\,k^n], \end{cases} \tag{2.5}$$

which in turn simplifies to

$$\begin{aligned} &(1/k + 2/k^{n-1}) + \left[\sum_{j=1}^{n-1} (n-1)!/[(n-j)!\,j!]\,(\varepsilon_1/k^n)^{j-1} (\delta_{n-1})^{n-j}\right] \times \\ &\times [M/k^{n-1} + \varepsilon_1/k^n (1/k + 2/k^{n-1})] \Big/ \prod_{i=1}^{n-1} \delta_i + (2/k^{n-1} + 1/k) \times \\ &\times \left\{\sum_{j=1}^{n-1} (n-1)!\Big/[(n-j)!\,j!]\,[\varepsilon_1 (2/k^n + 1/k^2)]^{j-1} (\delta_{n-1})^{n-j}\right\} \times \\ &\times [M + \varepsilon_1] \Big/ \prod_{i=1}^{n-1} \delta_i < k. \end{aligned}$$

Now using the fact that $k > 2$ we have that the last inequality will hold if

$$\begin{aligned} &3 + \left[\sum_{j=1}^{n-1} (n-1)!\Big/[(n-j)!\,j!]\,(\varepsilon_1)^{j-1} (\delta_{n-1})^{n-j}\right][M + 3\varepsilon_1] \Big/ \prod_{i=1}^{n-1} \delta_i + \\ &+ \left[3 \sum_{j=1}^{n-1} (n-1)!\Big/[(n-j)!\,j!]\,(3\varepsilon_1)^{j-1} (\delta_{n-1})^{n-j}\right][M + \varepsilon_1] \Big/ \prod_{i=1}^{n-1} \delta_i < k. \end{aligned}$$

However the quantity on the left in this last inequality is a fixed positive real number and the desired result follows.

LEMMA 2.2. *If*

$$|\psi_1(t)| \leqq \begin{cases} \exp\left(\lambda_n t - \varepsilon_1 t_0 + M(t-t_0)\right) & \text{for } t \geqq t_0, \\ \exp(\lambda_n t + \varepsilon_n t_0) & \text{for } t \leqq t_0 \end{cases}$$

$$|a_{ij}| < M, \quad \left|\int_0^t a_{ii}(\tau)\,d\tau - \lambda_i t\right| \leqq \begin{cases} \varepsilon_n t & \text{for } t \geqq t_0, \\ \varepsilon_n t_0 & \text{for } 0 \leqq t \leqq t_0 \end{cases} \quad \text{and}$$

$$\psi_{i1}(h) = \int_0^h \exp\left(\int_s^h a_{ii}(\tau)\,d\tau\right) a_{in}(s)\,\psi_1(s)\,ds \tag{2.6}$$

then

$$|\psi_{i1}(h)| \leqq (2M/\delta_{n-i}) \exp(\lambda_n h - \varepsilon_2 h) \quad \text{for} \quad a_1 t_0 \leqq h \leqq b t_0.$$

PROOF. From (2.6) we have

$$|\psi_{i1}(h)| \leqq M\int_0^{t_0} |\psi_1(s)| \exp\left(\int_s^h a_{ii}(\tau)\,d\tau\right) ds + M\int_{t_0}^h |\psi_1(s)| \exp\left(\int_s^h a_{ii}(\tau)\,d\tau\right) ds.$$

Considering the first term on the right we have

$$M\int_0^{t_0} |\psi_1(s)| \exp\left(\int_s^h a_{ii}(\tau)\,d\tau\right) ds \leqq M \exp(2\varepsilon_n h + \lambda_i h + \varepsilon_n t_0) \int_0^{t_0} \exp[(\lambda_n - \lambda_i)s]\,ds$$

$$< M/\delta_{n-i} \exp[2\varepsilon_n h + \lambda_i h + \varepsilon_n t_0 + (\lambda_n - \lambda_i) t_0] \leqq (M/\delta_{n-i}) \exp(\lambda_n h - \varepsilon_2 h)$$

provided that

$$(\delta_{n-i} + \varepsilon_n)/(\delta_{n-i} - \varepsilon_2 - 2\varepsilon_n)\, t_0 \leqq h.$$

Considering the second term on the right we have

$$M\int_{t_0}^h |\psi_1(s)| \exp\left(\int_s^h a_{ii}(\tau)\,d\tau\right) ds \leqq M \exp[2\varepsilon_n h + \lambda_i h - \varepsilon_1 t_0 + M(h - t_0)] \times$$

$$\times \int_{t_0}^h \exp[(\lambda_n - \lambda_i)\, s]\,ds < (M/\delta_{n-i}) \exp[h(2\varepsilon_n + \lambda_n + M) - t_0(\varepsilon_1 + M)]$$

$$< (M/\delta_{n-i}) \exp[h(\lambda_n - \varepsilon_2)] \quad \text{if} \quad [(M + \varepsilon_1)/(M + 2\varepsilon_n + \varepsilon_2)]\, t_0 > h.$$

This completes the proof of Lemma 2.2.

LEMMA 2.3. *If*

$$\psi_{ij}(h) = \int_0^h \exp\left(\int_s^h a_{ii}(\tau)\,d\tau\right) a_{in-j+1}(s)\,\psi_j(s)\,ds$$

and

$$|\psi_j(s)| \leqq \begin{cases} H \exp(-\varepsilon_j s + \lambda_n s) & \text{for } t_j \leqq s \leqq b_0 t, \\ \exp(\varepsilon_n t + \lambda_n s) & \text{for } 0 \leqq s \leqq t_j, \end{cases} \tag{2.7}$$

$$\left|\int_0^l a_{ii}(\tau)\,d\tau - \lambda_i l\right| \leqq \begin{cases} \varepsilon_n l & t_j \leqq l, \\ \varepsilon_n t_j & 0 \leqq l \leqq t_j, \end{cases} \tag{2.8}$$

$$[\delta_{n-i} + \varepsilon_n/(\delta_{n-i} - 2\varepsilon_n - \varepsilon_{j+1})]\, t_j \leqq h \leqq b_0 t, \tag{2.9}$$

then we have

$$|\psi_{ij}(h)| \leqq M\left(1/\delta_{n-i} + H/(\delta_{n-i} - \varepsilon_j)\right) \exp(\lambda_n h - \varepsilon_{j+1} h).$$

PROOF. From the definition of $\psi_{ij}(h)$ we have

$$|\psi_{ij}(h)| \leqq M\int_0^{t_j} |\psi_j(s)| \exp\left(\int_s^h a_{ii}(\tau)\,d\tau\right) ds + M\int_{t_j}^h \exp\left(\int_s^h a_{ii}(\tau)\,d\tau\right) |\psi_j(s)|\,ds.$$

Considering the first term on the right we have

$$M\int_0^{t_j}|\psi_j(s)|\exp\Big(\int_s^h a_{ii}(\tau)\,d\tau\Big)\,ds \leqq M\exp(2\varepsilon_n h+\varepsilon_n t_j+\lambda_i h)\times$$

$$\times\int_0^{t_j}\exp[(\lambda_n-\lambda_i)s]\,ds < (M/\delta_{n-i})\exp[2\varepsilon_n h+\varepsilon_n t_j+\lambda_i h+(\lambda_n-\lambda_i)t_j]$$

$$\leqq (M/\delta_{n-i})\exp(\lambda_i h-\varepsilon_{j+1}h) \text{ if } [(\delta_{n-i}+\varepsilon_n)/(\delta_{n-i}-2\varepsilon_n-\varepsilon_{j+1})]\,t_j \leqq h.$$

Considering the second term we have

$$M\int_{t_j}^{h}|\psi_j(s)|\exp\Big(\int_s^h a_{ii}(\tau)\,d\tau\Big)\,ds \leqq MH\exp(2\varepsilon_n h+\lambda_i h)\int_{t_j}^{h}\exp[(\lambda_n-\lambda_i-\varepsilon_j)s]\,ds$$

$$\leqq MH/(\delta_{n-i}-\varepsilon_j)\exp[(2\varepsilon_n+\lambda_n-\varepsilon_j)h] \leqq MH/(\delta_{n-i}-\varepsilon_j)\exp[\lambda_n h-\varepsilon_{j+1}h]$$

since $\varepsilon_{j+1}<\varepsilon_j-2\varepsilon_n$. This completes the proof of Lemma 2.3.

Proof of Theorem 2.1. The proof is by induction on n. For the case $n=1$ the result is immediate. We assume that the result holds for $n-1$ and establish it for n. Thus we have that for any $\varepsilon_n>0$ there exists $T(\varepsilon_n,0)$ such that

$$\begin{cases}\exp(\lambda_i t-\varepsilon_n t)\leqq\|[X(t,0)]_i\|\leqq\exp(\lambda_i t+\varepsilon_n t)\\ (t\geqq T(\varepsilon_n,0), \qquad i=1,\ldots,n-1)\end{cases} \tag{2.10}$$

$$\Big|\int_0^t a_{ii}(\tau)\,d\tau-\lambda_i t\Big|\leqq\begin{cases}\varepsilon_n t & [t\geqq T(\varepsilon_n,0),\ i=1,\ldots,n\\ \varepsilon_n T(\varepsilon_n,0) & [0\leqq t\leqq T(\varepsilon_n,0),\ i=1,\ldots,n-1.\end{cases} \tag{2.11}$$

Our result will be established if we cans how that given any $\delta_1/4>\varepsilon_1>0$ there exists $\overline{T}(\varepsilon_1,0)$ such that for $t\geqq\overline{T}(\varepsilon_1,0)$ we have

$$\Big|\int_0^t a_{nn}(\tau)\,d\tau-\lambda_n t\Big|\leqq\varepsilon_1 t. \tag{2.12}$$

We first establish that given any $\varepsilon_n>0$

$$\int_0^t a_{nn}(\tau)\,d\tau-\lambda t\leqq\varepsilon_n t \quad\text{for}\quad t>T(\varepsilon_n,0). \tag{2.13}$$

By (2.10) we have $\exp\Big(\int_0^t a_{nn}(\tau)\,d\tau\Big)=|[X_n(t,0)]_n|\leqq\|[X(t,0)]_n\|<\exp(\lambda_n t+\varepsilon_n t)$ for $t\geqq T(\varepsilon_n,0)$ and taking the log of both sides we have (2.13). We next establish that for any $\varepsilon_1>0$ and $t\geqq\max\Big[T(\varepsilon_n/2,0),\ 4\ln\Big(\sum_{i=1}^{n}K_i/\varepsilon_n\Big)\Big]=R$, we have

$$\int_0^t a_{nn}(\tau)\,d\tau-\lambda t\geqq-\varepsilon_1 t, \tag{2.14}$$

where ε_1 and ε_n are related as in Lemma 2.1 and

$$K_1=1,\quad K_j=2M/\delta_{j-1}+M\sum_{i=2}^{j-1}\big(1/\delta_{i-1}+K_i/(\delta_{j-1}-\varepsilon_i)\big)\quad\text{for}\quad 2\leqq j\leqq n.$$

For assume there existed a $t_0\geqq R$ such that

$$\int_0^{t_0}a_{nn}(\tau)\,d\tau<\lambda_n t_0-\varepsilon_1 t_0. \tag{2.15}$$

Now by (2.10) we have

$$(2.16)\quad 1\leqq \|[X(t,0)]_n\| \exp\left(-\lambda_n t+(\varepsilon_n/2)t\right)\leqq \sum_{j=1}^{n}|[X_j(t)]_n|\exp[(-\lambda_n+\varepsilon_n/2)t]$$

for $t\geqq R\geqq T(\varepsilon_n/2,0)$. We next observe that as a consequence of (2.15) we have that $\int_0^t a_{nn}(\tau)d\tau<\lambda_n t-\varepsilon_n t_0+(t-t_0)M$ for $t\geqq t_0$. Then by means of Lemmas 2.2 and 2.3 we have $|[X_{n-j+1}(h)]_n|\leqq K_j\exp(\lambda_n h-\varepsilon_j h)$ for any h such that $\left(\prod_{i=1}^{n-1}a_i\right)t_0\leqq h\leqq bt_0$. By Lemma 2.1 this set of values is nonvoid. Thus from (2.15) and (2.16) we have the existence of an $h>R$ such that

$$(2.17)\quad \begin{cases} 1\leqq \sum_{j=1}^{n}K_j\exp[(-\varepsilon_j+\varepsilon_n/2)h]\leqq \sum_{j=1}^{n}K_j\exp[(-\varepsilon_n/2)h] \\ \quad\leqq \sum_{j=1}^{n}K_j\exp\left((-\varepsilon_n/2)R\right)\leqq 1/2 \end{cases}$$

which is a contradiction. Thus if we take $\overline{T}(\varepsilon,0)=R$ we have our desired result and the proof of Theorem (2.1) is complete.

We next observe that the set $X(t,t_0)$ for $0\leqq t_0<\infty$ defines a one parameter family of fundamental solutions of system (2.2). We denote this family by $\mathscr{F}(s)$, $0\leqq s<\infty$, where $\mathscr{F}(t_0)=X(t,t_0)$. We shall say that $\mathscr{F}(s)$ has the set of S.C.E. $[\lambda_1,\ldots,\lambda_n]$ uniformly with respect to s if for any $\varepsilon>0$ there exists $T(\varepsilon)$ such that $|\ln\|[X(t+s,s)]_s\|-\lambda_i t|/t<\varepsilon$ for all $t\geqq T(\varepsilon)$ independently of s. We now have as an immediate consequence of Theorem 2.1 and its proof the following corollary.

COROLLARY 2.1. *If for system* (2.2) *the family* $\mathscr{F}(s)$ *has the set of* S.C.E. $(\lambda_1,\ldots,\lambda_n)$ *uniformly with respect to* s *where* $\lambda_i<\lambda_{i+1}$, $i=1,\ldots,n-1$ *then the functions* $a_{jj}(t)$ *satisfy condition* A *with means* λ_j *where* $j=1,\ldots,n$.

THEOREM 2.2. *If the diagonal terms* $a_{11}(t),\ldots,a_{nn}(t)$ *possess the distinct mean values* $\lambda_1,\ldots,\lambda_n$ *then system* (2.2) *possesses the* S.C.E. $[\lambda_1,\ldots,\lambda_n]$.

PROOF. The conclusion of the theorem is equivalent to the statement that system (2.2) possesses n independent solutions $\psi^i(t)$ such that for any $\varepsilon>0$ there exists m and M such that $m\exp(\lambda_i t-\varepsilon t)\leqq\|\psi^i(t)\|\leqq M\exp(\lambda_i t+\varepsilon t)$, $i=1,\ldots,n$. Before defining the desired $\psi^i(t)$ we introduce some necessary notation. If λ_i denotes the mean value of $a_{ii}(t)$ then we set $\overline{S}_i=\{l\,|\,l\leqq i,\ \lambda_l>\lambda_i\}$, and $S_i=\{l\,|\,l\leqq i,\ l\notin\overline{S}_i\}$. We now define the components of $\psi^i(t)$ as follows:

$$\psi_k^i(t)=0\qquad k\geqq i$$

$$\psi_i^i(t)=\exp\left(\int_0^t a_{ii}(s)\,ds\right)$$

$$\psi_k^i(t)=\begin{cases}\int_0^t \exp\left(\int_s^t a_{kk}(s)\,ds\right)\cdot\sum_{l=n}^{k+1}\psi_l^i(s)\,a_{kl}(s)\,ds & \text{if}\quad k\in S_i,\\ -\int_\infty^t \exp\left(\int_s^t a_{kk}(\sigma)\,d\sigma\right)\cdot\sum_{l=n}^{k+1}\psi_l^i(s)\,a_{kl}(s)\,ds & \text{if}\quad k\in\overline{S}_i.\end{cases}$$

We now show that for system (2.2) the above set of solutions satisfies the inequalities listed above. The case $n=1$ is immediate so we assume the result for $n-1$ and then obtain it for n. Now by the induction hypothesis we have that the solutions $\psi^i(t)$, $i=1, \ldots, n-1$ satisfy the given inequalities as do the last $(n-1)$ components of $\psi^n(t)$. Thus we need only show that for any $\varepsilon>0$ there exists an $M(\varepsilon)$ such that $|\psi_1^n(t)| \leqq M(\varepsilon)\exp(\lambda_n t+\varepsilon t)$ for $t\geqq 0$. If $\lambda_n-\lambda_1>0$ we take $\eta>0$ such that $4\eta<\min(\varepsilon, \lambda_n-\lambda_1)$, but if $\lambda_n-\lambda_1\leqq 0$ we take $\eta>0$ such that $4\eta<\varepsilon$. Then since the $a_{jj}(t)$ possess mean values λ_j and by our induction hypothesis there exists $M(\eta)$ such that

$$\left|\int_0^t a_{jj}(\tau)\,d\tau-\lambda_n t\right|<\eta t+\ln M(\eta), \qquad j=1, \ldots, n,$$

and

$$\sum_{l=2}^{n}|\psi_l^n(s)|\,|a_{nl}(s)| \leqq M(\eta)\exp(\lambda_n t+\eta t).$$

We then have the following bounds on $|\psi_1^n(t)|$ in the respective cases $n\in\bar{S}_1$ and $n\in\bar{S}_1$. If $n\in\bar{S}_1$,

$$\begin{aligned}|\psi_1^n(t)| &\leqq \int_{\infty}^{t} M\exp[\lambda_1(t-s)+2\eta s]\,M(\eta)\exp(\lambda_n s+\eta s)\,ds\\ &\leqq \exp(\lambda_n t+3\eta t)\,M^2(\eta)/\eta \leqq M^2\exp(\lambda_1 t+\varepsilon t)/\eta;\end{aligned}$$

while if $n\in S_1$,

$$\begin{aligned}|\psi_1^n(t)| &\leqq \int_{0}^{t} M(\eta)\exp[\lambda_1(t-s)+2\eta t]\,M(\eta)\exp(\lambda_n s+\eta s)\,ds\\ &\leqq M^2(\eta)\exp(3\eta t+\lambda_n t)/\eta \leqq M^2(\eta)\exp(\lambda_n t+\varepsilon t)/\eta;\end{aligned}$$

and our desired result follows.

COROLLARY 2.2. *A necessary and sufficient condition that system* (2.1) *possesses n distinct* S.C.E. $[\lambda_1, \ldots, \lambda_n]$ *is that it be kinematically similar to a super triangular system whose diagonal elements possess the mean values* $[\lambda_1, \ldots, \lambda_n]$.

COROLLARY 2.3. *A necessary and sufficient condition that for system* (2.2) *the family* $\mathfrak{F}(s)$ *has the set of* S.C.E. $[\lambda_1, \ldots, \lambda_n]$ *uniformly with respect to* s; *where* $\lambda_i<\lambda_{i+1}$, $i=1, \ldots, n-1$; *is that the functions* $a_{jj}(t)$; $j=1, \ldots, n$; *satisfy conditions* A *with means* λ_j.

To see that the above result is in a sense the best possible, we construct a two dimensional system which possesses the S.C.E. $[0, 0]$, i.e. has multiple characteristic exponents, and for which there is an upper triangular representation in which one of the diagonal terms fails to possess a mean value. In preparation for this example we have the following lemma.

LEMMA 2.4. *There exists a positive real valued function* $f(t)$ *such that* $\lim_{t\to\infty}(\ln f(t)/t)=-1/2$, $\overline{\lim_{t\to\infty}}(\ln f(t)/t)=0$, $\lim_{t\to\infty}\left(\ln\int_0^t f(s)\,ds/t\right)=0$ *and* $g(t)=\int_0^t f(s)\,ds$ *assumes arbitrarily large values for sufficiently large* t.

PROOF. We define $f(t)$ as follows. Let $t_0=0$, t_1 a given positive number, and t_i be given by the recursive formula $t_{i+1}=8t_i$ for $i\geqq 1$; then we have

$$f(t)=1 \quad \text{for} \quad t\in(4t_i, t_{i+1}) \quad \text{and} \quad i=0,1,\ldots,$$

$$f(t)=\exp(t_i-t) \quad \text{for} \quad t\in(t_i, 2t_i) \quad \text{and} \quad i=1,2,\ldots,$$

$$f(t)=\exp\big(-2t_i+(t-2t_i)\big) \quad \text{for} \quad t\in(2t_i, 4t_i) \quad \text{and} \quad i=1,2,\ldots.$$

Since $f(2t_i)=\exp(-t_i)$ and $f(4t_i)=1$ it follows that $\underline{\lim}_{t\to\infty}\big(\ln f(t)/t\big)=-1/2$ and $\overline{\lim}_{t\to\infty}\big(\ln f(t)/t\big)=0$. It is also readily verified that $t>\int_0^t f(s)\,ds\geqq t/4$ for all t and so $\lim_{t\to\infty}(\ln g(t)/t)=0$. Since $f(t)$ is always equal to or greater than zero $g(t)$ is a positive monotone, and in fact, unbounded increasing function of t. This completes the proof of Lemma 2.4.

EXAMPLE 2.1. Define $K(t)=\frac{d}{dt}[\ln f(t)]$ at all points except $t=t_i, t_{2i}$ and t_{4i} where $i=0, 1, 2, \ldots$, and at these exceptional points set $K(t)=0$. Then the system $\dot{x}=C(t)\,x$ where $C(t)=\begin{pmatrix}0 & 1\\ 0 & K(t)\end{pmatrix}$ has the set of fundamental solutions

$$\begin{pmatrix}C_1\int_0^t f(\tau)\,d\tau+C_2\\ 0 \qquad\qquad f(t)\end{pmatrix} \qquad (-\infty<C_1, C_2<\infty)$$

and so this system has the S.C.E. $[0, 0]$. Our example has the disadvantage that the function $K(t)$ is not continuous everywhere. Since, however, $K(t)$ is a step function with isolated discontinuities it is clear that we could redefine $K(t)$ in such a way that it was continuous and still preserve the properties of its integral $f(t)$ as described above. Once this modification has been carried out we obtain an example of a system which possesses a pair of strong characteristic exponents but at the same time has an upper triangular representation in which the diagonal terms do not all possess mean values.

Section 3. Stability Theory

In this section we consider the system of the form

$$\dot{x}=[D+B(t)]\,x+f(t, x) \tag{3.1}$$

where

1. $\|f(t, x_1)-f(t, x_2)\|=o\big(\|x_1-x_2\|\big)$ when $\|x_1\|$, $\|x_2\|$ tend to zero,
2. $D=\operatorname{diag}(d_{11}, \ldots, d_{nn})$ $(d_{11}\leqq d_{22}\leqq\cdots\leqq d_{nn})$, $d_{kk}<0$,
3. if $\delta=\min_{d_i\neq d_{jj}}|d_i-d_{jj}|$ then $\|B(t)\|<\delta/(16n)$.

THEOREM 3.1. *For $t=0$ there exists in the x space a real k dimensional manifold S_k containing the origin such that any solution φ of (3.1) with $\varphi(0)$*

on the manifold S_k tends to zero at an exponential rate of at least $d_{kk}+\delta/2$. Moreover, the manifold S_k is differentiable if $\partial f/\partial x_i$ exists and is continuous for $i=1, \ldots, n$ and $t \geqq 0$.

PROOF. This result is a generalization of the author's result [4] for linear systems and of Theorems 4.1 and 4.3 found in CODDINGTON and LEVINSON [1]. For this reason we shall use notation which is analogous to that employed in the latter case. Thus if j is the smallest integer such that $d_{j+1\,j+1} > d_{kk}$ we define

$$U_1(t) = \operatorname{diag}[\exp(d_{11}t), \ldots, \exp(d_{jj}t), 0, \ldots, 0)]$$

and

$$U_2(t) = \exp(Dt) - U_1(t).$$

Now let a denote any point in the x space whose last $n-k$ components are zero [i.e., $a=(a_1, \ldots, a_k, 0, 0, \ldots, 0)$]. We now show that there exists a $\gamma>0$ such that for $\|a\|<\gamma$ we may define a continuous vector valued function $\vartheta(t, a)$ such that $\vartheta_i(0, a)=a_i$, $i \leqq k$, and the remaining components $\vartheta_i(0, a)=y_i$, $i>k$, define for us the desired k dimensional manifold. Thus we consider the integral equation

$$(3.2)\quad \vartheta(t, a) = U_1(t)\,a + \int_0^t U_1(t-s)\,g\big(s, \vartheta(s, a)\big)\,ds - \int_t^\infty U_2(t-s)\,g\big(s, \vartheta(s, a)\big)\,ds$$

where a is a constant vector and $g\big(s, \vartheta(s, a)\big) = B(s)\,\vartheta(s, a) + f\big(s, \vartheta(s, a)\big)$. Let $\gamma_1>0$ be chosen so that for $\|\vartheta^i(s, a)\|<\gamma_1$, $i=1, 2$, we have

$$\|g\big(s, \vartheta^1(s, a)\big) - g\big(s, \vartheta^2(s, a)\big)\| \leqq (\delta/8n)\,\|\vartheta^1(s, a) - \vartheta^2(s, a)\|.$$

By conditions 1. and 3. this is clearly possible. Setting $\gamma=\gamma_1/2$ and using successive approximations to solve (3.2) with $\vartheta^0(t, a)=0$, it follows that

$$\|\vartheta^{j+1}(t, a) - \vartheta^j(t, a)\| \leqq \|a\| \exp[(d_{kk} + \delta/2)\,t]/4^j.$$

This leads to the existence of a solution $\vartheta(t, a)$ of (3.2) which satisfies

$$\|\vartheta(t, a)\| \leqq 2\gamma \exp[(d_{kk} + \delta/2)\,t].$$

The continuity of $\vartheta(0, a)$ follows from the uniform convergence and the continuity of the $\vartheta^j(0, a)$. The proof of the results in the last two statements are straightforward generalizations of the proofs of similar statements in Theorems 4.1 and 4.2 referred to above, and will not be displayed here. We note finally that the first restriction on $f(t, x)$ may be weakened to $f(t, x)=o\big(\|x\|\big)$ as $\|x\|$ tends to zero. In this case the successive approcimations for the solution of (3.2) will not necessarily converge directly, but we must use the fact that they define an equicontinuous uniformly bounded family and so one may select a convergent subsequence. That this is the case is established by noting that

$$\|\vartheta^1\| \leqq 2(1 - 1/2^1)\,\gamma \exp[(d_{kk} + \delta/2)\,t],$$

and then assuming that

$$\|\vartheta^j\| \leqq 2(1 - 1/2^j)\,\gamma \exp[(d_{kk} + \delta/2)\,t]$$

we obtain

$$\|\vartheta^{l+1}\| \leqq 2(1-1/2^{l+1})\gamma \exp[(d_{kk}+\delta/2)t].$$

Thus

$$\|\vartheta\| \leqq 2\gamma \exp[(d_{kk}+\delta/2)t]$$

and things proceed as before. Thus we have

THEOREM 3.2. *The conclusions of Theorem* 3.1 *hold where the restriction* 1. *in the definiton of* (3.1) *is replaced by the weaker condition that*

$$f(x,t) = o(\|x\|) \quad as \quad \|x\| \to 0.$$

Section 4. Approximate Similarity

When MARKUS [5] and others considered the concept of kinomatic similarity, the strongest perturbation theorems available were those which insisted that the nonlinear perturbation $f(x,t)$ satisfy a restriction of the form $f(x,t) = o(\|x\|)$ uniformly in t. Thus, in their definition of equivalence it was necessary to restrict oneself to an equivalence relationship which would preserve this condition. The results of Section 3, however, make it possible in many cases to relax the notion of equivalence and still have equivalent systems possessing the same stability properties. Thus we introduce the concept of approximate similarity.

DEFINITION 4.1. *The matrix* $A(t) \in M_n$ *is said to be approximately similar to* $B(t) \in M_n$, *written* $A \approx B$, *if given any* $\varepsilon > 0$ *there exists a* $P(\varepsilon, t)$ *such that*

$$P(\varepsilon,t),\ P^{-1}(\varepsilon,t),\ \dot{P}(\varepsilon,t) \in M_n \quad and \quad \|P^{-1}(-\dot{P}+A(t)P) - B(t)\| < \varepsilon.$$

We now have a number of observations about approximate similarity.

[4.1] The relation of approximate similarity is a transitive and reflexive relation.

[4.2] The set of all matrices in M_n to which $A(t)$ is approximately similar, written $E(A)$, is a closed set.

[4.3] For every $A \in M_n$ the set $E(A)$ contains at least one diagonal matrix.

[4.4] If $E(A)$ contains a diagonal matrix of constant terms, $\lambda_1, \lambda_2, \ldots, \lambda_n$, not necessarily distinct, then the system $\dot{x} = A(t)x$ possesses the S.C.E. $[\lambda_1, \ldots, \lambda_n]$.

[4.5] By Perron's classical example we have that there exist $A, B \in M_n$ such that $A \approx B$ and the systems $\dot{x} = A(t)x$ and $\dot{y} = B(t)y$ possess different sets of characteristic exponents.

[4.6] Every constant matrix A is approximately similar to a constant diagonal matrix where the diagonal terms are the real parts of the characteristic roots of $\det |A - \lambda I|$.

[4.7] Every periodic matrix $P(t)$ is approximately similar to a constant diagonal matrix where the diagonal terms are just the characteristic exponents of the system $\dot{x} = P(t)x$.

For certain applications it is of particular interest to have an idea of the size of the set of matrices $A \in M_n$ for which $A \approx C$, C being a constant matrix. Our main result in this connection is found in Corollary 4.1. In preparation for this result and Theorem, 4.1 we have the following algebraic lemma.

LEMMA 4.1. *Given two sets of elements A_i and σ_i $(\sigma_i > 0,\ i = 1, \ldots, n)$ which satisfy the inequalities*

$$\sum_{i=k}^{l} (A_i + \sigma_i \mu) \geqq -M, \quad 1 \leqq k \leqq l \leqq n, \tag{4.1}$$

$$\sum_{i=k}^{l} (A_i - \sigma_i \mu) \leqq M, \quad 1 \leqq k \leqq l \leqq n, \tag{4.2}$$

where $M > 0$, $\mu > 0$, then there exists a third set μ_i, $|\mu_i| < \mu$, $i = 1, \ldots, n$ such that

$$-M \leqq \sum_{i=k}^{l} A_i + \mu_i \sigma_i \leqq M \quad 1 \leqq k \leqq l \leqq n. \tag{4.3}$$

PROOF. The proof is by induction on the number of elements in the set. Before proceeding to the induction we introduce some notation. We shall denote the sum $\sum_{i=k}^{l} (A_i + \mu_i \sigma_i)$ by $H(k, l)$ or $H(\mu_k, \ldots, \mu_l)$ where $|\mu_i| \leqq \mu$ for $k \leqq i \leqq l$; the inequality $-M \leqq H(k, l) \leqq M$ is denoted by $I(k, l)$, or by $I(\mu_k, \ldots, \mu_l)$ if particular values of the μ_i are to be indicated. Likewise $S(k, l)$ or $S(\mu_k, \ldots, \mu_l)$ denotes the set of all the $I(j, h)$ or $I(\mu_j, \ldots, \mu_h)$, respectively, where $k \leqq j \leqq h \leqq l$. We denote the total set of values $(\mu_k, \ldots, \mu_l)$ which satisfy the inequalities $S(k, l)$ as $\Delta(k, l)$, and the interval $(-\mu, \mu)$ by Δ. Also we have $\sigma(k, l) = \sum_{i=k}^{l} \sigma_i \mu_i$ where $(\mu_k, \ldots, \mu_l) \in \Delta(k, l)$, $\bar{\sigma}(k, l) = \max \sigma(k, l)$, $\underline{\sigma}(k, l) = \min \sigma(k, l)$, and the associated values for which the extremes are assumed by $\bar{\mu}(k, l) = (\bar{\mu}_k, \ldots, \bar{\mu}_l)$ and $\underline{\mu}(k, l) = (\underline{\mu}_k, \ldots, \underline{\mu}_l)$, respectively. Finally we have that the restriction of $(\mu_k, \ldots, \mu_l)$ to $(\mu_j, \ldots, \mu_h)$ will be written $(\mu_k, \ldots, \mu_l) | (j, h)$.

We now proceed with the induction. For the case $n = 1$ the result is immediate. We now assume the result for all sets of $n - 1$ elements and establish it for the case of n elements. Thus we consider the two sets A_i, σ_i, $i = 1, \ldots, n$. By the induction hypothesis the sets $\Delta(1, n-1)$ and $\Delta(2, n)$ are nonempty, and we now establish that the intersection $\Delta \times \Delta(2, n) \cap \Delta(1, n-1) \times \Delta$ is also nonempty. We first observe that if there exists μ_1, $|\mu_1| \leqq \mu$, such that $A_1 + \mu_1 \sigma_1 = 0$, then $\mu_1 \times \Delta(2, n)$ has the desired property and we have our result. The proof proceeds similarly if there exists a μ_n such that $A_n + \mu_n \sigma = 0$. Thus we are reduced to four cases.

Case 1. $A_1 + \mu \sigma_1 < 0$ and $A_n + \mu \sigma_n < 0$,

Case 2. $A_1 + \mu \sigma_1 < 0$ and $A_n - \mu \sigma_n > 0$,

Case 3. $A_1 - \mu \sigma_1 > 0$ and $A_n - \mu \sigma_n < 0$,

Case 4. $A_1 - \mu \sigma_1 > 0$ and $A_n - \mu \sigma_n > 0$.

We consider first cases 1 and 2. Now in both of these cases we see that for any point $\xi \in \Delta \times \Delta(2, n)$ the inequalities $S(2, n)$ hold along with the inequalities $S(1, n-1)$ on the right side. Thus we need only show that there exists a point in $\Delta \times \Delta(2, n)$ such that the inequalities $S(1, n-1)$ hold on the left. Consider the point $\mu \times \bar{\mu}(2, n)$, then for this point we must either have one of the equalities $H((\bar{\mu}_2, \ldots, \bar{\mu}_n) | (j, k)) = M$ where $2 \leqq j \leqq k \leqq n$, or else $(\bar{\mu}_2, \ldots, \bar{\mu}_n) = (\mu, \ldots, \mu)$; and in the latter case, $H(1, n) = H(\mu, \ldots, \mu) \geqq -M$ is a consequence of inequality 4.1. Thus we may assume that the value M is actually assumed, say $H(\bar{\mu}_j, \ldots, \bar{\mu}_l) = M$ where j is the smallest index for which this occurs. Now we note that μ_r, $2 \leqq r < j$, in $(\bar{\mu}_2, \ldots, \bar{\mu}_n)$ must be μ, in light of definition $\bar{\sigma}(2, n)$. We now establish that $-M \leqq H(\mu, \bar{\mu}_2, \ldots, \bar{\mu}_s)$ for all $2 \leqq s \leqq n$. For $s \leqq j-1$ we have by 4.1 that $H(\mu, \bar{\mu}_2, \ldots, \bar{\mu}_s) = H(\mu, \ldots, \mu) \geqq -M$, and for $s \geqq l$ we have $H(\mu, \bar{\mu}_2, \ldots, \bar{\mu}_s) = H(\mu, \bar{\mu}_2, \ldots, \bar{\mu}_{j-1}) + H(\bar{\mu}_j, \ldots, \bar{\mu}_l) + H(\bar{\mu}_{l+1}, \ldots, \bar{\mu}_s) \geqq -M + M - M = -M$. For $j \leqq s \leqq l$ we notice that $H(\bar{\mu}_j, \ldots, \bar{\mu}_l) = H(\bar{\mu}_j, \ldots, \bar{\mu}_s) + H(\bar{\mu}_{s+1}, \ldots, \bar{\mu}_l)$. But since $H(\bar{\mu}_j, \ldots, \bar{\mu}_l) = M$ and $H(\bar{\mu}_{s+1}, \ldots, \bar{\mu}_l) \leqq M$ we have that $H(\bar{\mu}_j, \ldots, \bar{\mu}_s) \geqq 0$. Thus $H(\mu, \bar{\mu}_2, \ldots, \bar{\mu}_s) = H(\mu, \bar{\mu}_2, \ldots, \bar{\mu}_{j-1}) + H(\bar{\mu}_j, \ldots, \bar{\mu}_s) \geqq -M$, and so in all cases $(\mu, \bar{\mu}_2, \ldots, \bar{\mu}_n)$ satisfies all the inequalities $S(2, n)$ and $S(1, n-1)$. In cases 3 and 4 the argument is similar except that M is replaced by $-M$, μ by $-\mu$, $(\bar{\mu}_2, \ldots, \bar{\mu}_n)$ by $(\underline{\mu}_2, \ldots, \underline{\mu}_n)$, and the problem is to establish the inequalities $S(1, n-1)$ on the right. Thus the set of points $S = \{(\gamma_1, \ldots, \gamma_n)$ such that the inequalities $S(2, n)$ and $S(1, n-1)$ are jointly satisfied$\}$ is nonempty. We let $(\bar{\gamma}_1, \ldots, \bar{\gamma}_n)$ be any point in S such that $\sum_{i=1}^{n} \gamma_i \sigma_i$ is a maximum and $(\underline{\gamma}_1, \ldots, \underline{\gamma}_n)$ be any point of S such that $\sum_{i=1}^{n} \gamma_i \sigma_i$ is a minimum. We now show that $H(\underline{\gamma}_1, \ldots, \underline{\gamma}_n) \leqq M$ and $H(\bar{\gamma}_1, \ldots, \bar{\gamma}_n) \geqq -M$. Then, since the set S is convex, it will follow that for some point $(\gamma_1, \ldots, \gamma_n) \in S$ on the line from $(\bar{\gamma}_1, \ldots, \bar{\gamma}_n)$ to $(\underline{\gamma}_1, \ldots, \underline{\gamma}_n)$ we have $-M \leqq H(\gamma_1, \ldots, \gamma_n) \leqq M$ which will in turn complete our induction. We first establish that $H(\bar{\gamma}_1, \ldots, \bar{\gamma}_n) \geqq -M$. Now either for some (j, l), $1 \leqq j \leqq l \leqq n-1$ or $2 \leqq j \leqq l \leqq n$, we have $H(\bar{\gamma}_j, \ldots, \bar{\gamma}_l) = M$, or else $(\bar{\gamma}_1, \ldots, \bar{\gamma}_n) = (\mu, \ldots, \mu)$ in which case our inequality is a consequence of 4.1. If $H(\bar{\gamma}_j, \ldots, \bar{\gamma}_l) = M$, then we have

$$H(\bar{\gamma}_1, \ldots, \bar{\gamma}_n) = H(\bar{\gamma}_1, \ldots, \bar{\gamma}_{j-1}) + H(\bar{\gamma}_j, \ldots, \bar{\gamma}_l) + H(\bar{\gamma}_{l+1}, \ldots, \bar{\gamma}_n)$$
$$\geqq -M + M - M = -M.$$

The proof that $H(\underline{\gamma}_1, \ldots, \underline{\gamma}_n) \leqq M$ is similar where $\underline{\gamma}_i$ replace $\bar{\gamma}_i$, $-M$ replaces M, and $-\mu$ replaces μ. This then completes our induction and so the proof of Lemma 4.1.

THEOREM 4.1. *If* $|a(s)| \leqq M_3$, $-\infty < s < \infty$, *and for every* $\mu > 0$ *there exists a constant* $M(\mu)$ *such that* $\int_s^t a(\tau)\, d\tau \leqq M(\mu) + \mu |t - s|$, $-\infty < s, t < \infty$, *then there exists a continuous function* $\mu(t)$ *such that* $|\mu(s)| \leqq \mu$ *and*

$$\int_s^t [a(\tau) - \mu(\tau)]\, d\tau \leqq M(\mu)[3 + 2M_3/\mu] + \mu^2, \quad -\infty < s, \quad t < \infty.$$

PROOF. We may without loss of generality assume $2\mu < M(\mu)/M_3$. We consider first the interval $(-k, k)$, k a positive integer, and associate with it a partition with division points t_i where $t_0 = -k$, and for any $i > 0$ such that $t_{i-1} < k$, we set $t_i = \min(t_{i-1} + \sigma_i, k)$. Here $\sigma_i = \min\{M(\mu)/\mu,\ s \in S_i\}$ where $S_i = \left\{\{s \mid s \geqq 0,\ \left|\int_{t_{i-1}}^{t_{i-1}+s} a(\tau)\,d\tau\right| = M\right\}$. The t_i clearly define a partition of $(-k, k)$ into a finite number of parts, say n. Setting $A_i = \int_{t_{i-1}}^{t_i} a(s)\,ds$ we have by Lemma 4.1 that there exists a set of real numbers μ_i, $|\mu_i| < \mu$, such that

$$\left|\sum_{i=l}^{k} (A_i + \mu_i \sigma_i)\right| \leqq M(\mu) \quad \text{for} \quad 1 \leqq l \leqq k \leqq n.$$

Setting $\mu_0 = 0$, $\mu_{n+1} = 0$, and $\Delta_i = \mu_{i+1} - \mu_i$, we now define the function $\mu_k(t)$ as follows

$$\mu_k(t) = 0, \quad (-\infty < t < t_0 - |\Delta_0|/2)$$

$$\mu_k(t) = \mu_i, \quad (t_{i-1} + |\Delta_{i-1}|/2 < t < t_i - |\Delta_i|/2,\ i = 1, \ldots, n)$$

$$\mu_k(t) = \mu_i + \Delta_i\{t - (t_i - |\Delta_i|/2)\}/|\Delta_i|, \quad (t_i - |\Delta_i|/2 \leqq t \leqq t_i + |\Delta_i|/2,\ i = 0, 1, \ldots, n)$$

$$\mu_k(t) = 0, \qquad (t_n + |\Delta_n|/2 \leqq t < \infty).$$

Consider now the family of functions $\{\mu_k(t)\}$, $k = 1, 2, \ldots$. This clearly is a uniformly bounded and equicontinuous family. Thus we may select a convergent subsequence $\{\mu_i(t)\}$ which converges on every finite interval to a limit function $\mu(t)$. We assert that $\mu(t)$ satisfies the conditions of our theorem. The condition $|\mu(s)| \leqq \mu$, $-\infty < s < \infty$ is clearly satisfied, and it only remains to establish the second condition for any fixed $-\infty < s \leqq t < \infty$. For any fixed s, t and $\varepsilon > 0$ we may take the index l in the subsequence $\{\mu_i(t)\}$ so large that $-l \leqq s,\ t \leqq l$ and $\int_s^t |\mu(\sigma) - \mu_l(\sigma)|\,d\sigma < \varepsilon$. Then if we set t_r = largest t_i and t_m = smallest t_i in the partition of $(-l, l)$ such that $t_r \leqq t$ and $t_m \geqq s$, we have

$$\left|\int_s^t [a(\tau) - \mu(\tau)]\,d\tau\right| \leqq \left|\int_s^t [a(\tau) - \mu_l(\tau)]\,d\tau\right| + \int_s^t |\mu(\sigma) - \mu_l(\sigma)|\,d\sigma$$

$$\leqq \left|\int_{t_m}^{t_r} [a(\tau) - \mu_l(\tau)]\,d\tau\right| + \left|\int_{t_r}^{t} [a(\tau) - \mu_l(\tau)]\,d\tau\right| +$$

$$+ \left|\int_{s}^{t_m} [a(\tau) - \mu_l(\tau)]\,d\tau\right| + \varepsilon \leqq M(\mu) + \mu^2 + 2(M_3 + \mu)(M(\mu)/\mu) + \varepsilon.$$

Now letting $l \to \infty$ we have our desired result.

COROLLARY 4.1. *If $A(t)$ is approximately similar to a diagonal matrix each of whose terms possesses property A^+ then $A(t)$ is approximately similar to a diagonal matrix of constants.*

5. Applications

In this section we shall consider an n-dimensional system of the form

$$\dot{x} = F(x, \mu, t). \tag{5.1}$$

DEFINITION 5.1. *System* 5.1 *is said to possess property I with respect to a bounded curve* $p(0, t)$ *if there exists a* $\Delta \geqq 0$ *such that for* $0 < |\mu|$, $\|\eta\| \leqq \Delta$ *it may be written in the form*

$$\dot{\eta} = F\left(p(0,t), \mu, t\right) - F\left(p(0,t), 0, t\right) + \left[A(\mu, t) + \mathscr{F}(\eta, \mu, t)\right]\eta \tag{5.2}$$

where

1. $\eta = x - p(0, t)$

2. $\mathscr{F}_{qi} = \sum_{j=1}^{n} \left[F^q_{x_i x_j}\left(p(0,t), \mu, t\right) + F^q_{x_i x_j}\left(p(0,t) + \vartheta(t, \eta)\eta, \mu t\right)\right]\eta_j$

where F^q *is the q-th component of the vector function* $F(x, \mu, t)$ *and* $|\vartheta_{ij}(t, \eta)| < 1$,

3. $A(\mu, t)$ *and* $F^q_{x_i x_j}$ $(i, j, q = 1, \ldots, n)$ *are bounded, continuous in* x, μ, t *and jointly continuous in* μ, x *uniformly for* $-\infty < t < \infty$,

4. $A(0, t)$ *is approximately similar on the infinite interval to a real constant diagonal matrix* D *none of whose terms vanish.*

For systems of this form the author has established the following result [3].

THEOREM 5.1. *If system* (5.1) *possesses property I with respect to a bounded curve* $p(0, t)$, *then there exists a* $\Delta > 0$ *such that to every* μ, $|\mu| < \Delta$, *there corresponds a bounded solution* $p(\mu, t)$ *of* (5.1). *The solution* $p(\mu, t)$ *tends to* $p(0, t)$ *uniformly as* μ *tends to zero.*

DEFINITION 5.2. *Two bounded solution curves* $p(\mu, t)$ *and* $p(\mu_2, t)$ *of* (5.1) *will be said to possess the same stability properties if there exist* $\delta > 0$ *and an integer* k *such that for* $t = 0$ *there corresponds to each* $p(\mu_i, t)$ *a unique* k *dimensional manifold* S_{ki} *containing the point* $p(\mu_i, 0)$ *and such that solutions starting on this manifold tend asymptotically towards* $p(\mu_i, t)$, $i = 1, 2$. *We further insist that any solution* $x(\mu_i, t)$ *such that* $\|x(\mu_i, 0) - p(\mu_i, 0)\| < \delta$, $x(\mu_i, 0) \notin S_{ki}$, *must for some* $t > 0$ *satisfy* $\|x(\mu_i, t) - p(\mu_i, t)\| > \delta$.

As an immediate consequence of Theorem 5.1 and Section 3 we have

THEOREM 5.2. *There exists* $\sigma > 0$ *such that, if in Theorem 5.1 we set* $\Delta = \sigma$, *then the solutions* $p(\mu, t)$ *described in Theorem 5.1 possess the same stability properties.*

Bibliography

[1] CODDINGTON, E., and N. LEVINSON: Theory of Ordinary Differential Equations. New York: McGraw-Hill 1955. — [2] DILIBERTO, S.: On Systems of Ordinary Differential Equations, Contributions to the Theory of Non-linear Oscillations, S. Lefschetz, ed.: 1–39. Princeton University Press 1950. — [3] LILLO, J.: Stability Theory, Technical Report, Ordnance Research, U.S.Army Contract No. DA-23-072-ORD-1289, University of Kansas. — [4] LILLO, J.: On almost periodic solutions of differential equations. Annals of Math. **69**, 1–19 (1955). — [5] MARKUS, L.: Continuous matrices and the stability of differential systems. Math. Z. **62**, 310–319 (1955). — [6] PERRON, O.: Die Ordnungszahlen linearer Differentialgleichungssysteme. Math. Z. **31**, 748–766 (1930).

Dept. of Math., University of Kansas, Lawrence, Kansas (USA)

(Eingegangen am 24. April 1959)

BRUCK, R. H.
Math. Zeitschr. 73, 59–78 (1960)

Some Theorems on Moufang Loops

By
R. H. BRUCK[1])

1. INTRODUCTION. The present paper is concerned with several loosely allied topics in loop theory with special reference to Moufang loops. That the topics are included under one heading may best be explained by the fact that, to a considerable extent, progress in any one of the topics depends on progress in the others. The main purpose of this introduction is to provide the connecting links.

We begin by considering the *isotopy-isomorphy problem: For what loops G is it true that every loop isotopic to G is isomorphic to G?* As shown in [*1*], this is a question of considerable geometric significance, particularly in relation to 3-nets. If we add the assumption that G is a Moufang loop then (See [*1*], Chapter VII, Theorem 2.3) a necessary and sufficient condition that every loop isotopic to G be isomorphic to G is that every element of G be a companion of at least one pseudo-automorphism of G. This brings us to the study of the companions of the pseudo-automorphisms of a Moufang loop G. In § 2 we are able to prove that (a) *NG^3 is a normal subloop of G* (Theorem 2.1) and that (b) *every element of NG^3 is a companion of some pseudo-automorphism of G* (Theorem 2.2). Here N is the nucleus of G and G^3 is the subloop generated by all cubes of elements of G. In view of (b) we may state:

THEOREM 1.1. *If G is a Moufang loop with nucleus N such that $G=NG^3$, then every loop isotopic to G is isomorphic to G.*

Now let us assume that G is a simple Moufang loop. In view of (a), we must have either (i) $G=NG^3$ or (ii) $NG^3=1$. We should like to dispose of (ii). In order to do so, we need to study Moufang loops of exponent 3; and indeed, in § 5, we consider the slightly wider class of Moufang loops which satisfy the identical relation

$$(x\,y)^3 = x^3\,y^3. \tag{1.1}$$

In particular, by Corollary 2 of Theorem 5.2, *if G is a simple Moufang loop such that $G^3=1$ then either $G=1$ or G is the group of three elements.* In either case, $G=N=NG^3$. Hence:

THEOREM 1.2. *If G is a simple Moufang loop with nucleus N, then* (i) *$G=NG^3$ and* (ii) *every loop isotopic to G is isomorphic to G.*

By considering the multiplicative (Moufang) loop of regular elements of a simple 8-dimensional alternative algebra in the light of Theorems 1.1, 1.2, one could probably give a new proof of the isotopy-isomorphy theorem for

[1]) This research was supported in part by a grant from the National Science Foundation.

simple alternative rings. This, however, would be at most a non-essential application of loop theory to ring theory.

To go much further in the direction of Theorems 1.1, 1.2 we would need to know more about the companions of pseudo-automorphisms. For example, *do the companions of pseudo-automorphisms of a Moufang loop G from a subloop of G?* A start upon this problem is given in Lemma 2.2 (which is also needed for the proof of Theorem 2.2). For further progress it would seem helpful to study the companions of pseudo-automorphisms of G/G^3. (By Theorem 2.1, G^n is a normal subloop of G for every integer n.) Since G/G^3 is a Moufang loop of exponent 3, we are again back to the Moufang loops satisfying (1.1).

We might recall that if G is a commutative loop (not assumed to be Moufang) with the property that every loop isotopic to $\hat{G}$ is isomorphic to G, then G is an abelian group. (This is the loop analogue of the geometric fact that Pappus' Theorem implies Desargues' Theorem.) Since there exist commutative Moufang loops which are not abelian groups, not every Moufang loop has the isotopy-isomorphy property.

Before turning to other topics, it seems appropriate to acknowledge a communication from J. Tits which set me on the track of Theorem 1.1. Tits proved (in slightly different language and by different methods) that *if G is a Moufang loop with nucleus N and if s is an element of G whose square is in N, then s is a companion of some pseudo-automorphism of G.* He showed that, if S is the set of such elements s, then all products of type

$$s_1 \cdot \left(s_2 \cdot (\ldots (s_{k-1} \cdot s_k) \ldots)\right), \qquad s_1, \ldots, s_k \in S,$$

are also companions. Note, however, that if s^2 is in N then s is in NG^3. Thus Tits' result is a corollary of Theorem 2.2.

In preparing to study the class of all Moufang loops satisfying (1.1) we are guided by two considerations: (i) the class contains the commutative Moufang loops and the structure of these is well developed; (ii) every Moufang loop satisfying (1.1) is either an isotope of a commutative Moufang loop or a normal subloop of index 3 in such a loop-isotope. [For (ii), see Theorem 5.1.] In view of (ii) we begin (in § 3) with a study of isotopic invariants. In addition, since every commutative Moufang loop is locally centrally nilpotent, we restrict attention to nilpotency properties and to finiteness properties. There is no need at this point, however, to restrict ourselves to Moufang loops.

Our main results are as follows: (1) *If G is a loop with a central system of given order type, every loop isotopic to G has a central system of the same order type* (Theorem 3.1). (2) *The properties of being locally finite or locally centrally nilpotent are isotopic invariants* (Theorem 3.2).

The results (1), (2) are sufficient to allow us to carry over at least some of the properties of commutative Moufang loops to the Moufang loops satisfying (1.1). However, we wish to parallel the known structure theory of commutative Moufang loops as closely as possible (and finally do, in Theorem 5.2). At several points we encounter the following difficulty: we are given a Moufang loop G with centre Z and wish to deduce certain properties of G from properties

of G/Z. We solve the problem (in § 4) for the class of di-associative loops (which contains all Moufang loops) by proving the following: *If G is a di-associative loop with centre Z such that G/Z is locally finite, and if P is the set of all elements of G of finite order, then P is a locally finite normal subloop of G and G/P is an abelian group* (Theorem 4.3). The proof of Theorem 4.3 uses the fact that the commutator-asserciator subloop G' is locally finite (Theorem 4.2); note however that if G/P is an abelian group, P contains G'. Another contributing theorem has an interest in its own right: *If G is a di-associative loop such that G/Z is finite, then G' is finite* (Theorem 4.1).

With this much equipment we are in a position to prove the main theorem (Theorem 5.2) concerning the Moufang loops satisfying (1.1). We merely remark here that Theorem 5.2 is, at one and the same time, a type of "Burnside" theorem for the Moufang loop G satisfying (1.1), the multiplication group of G and the inner mapping group of G.

In the concluding section (§ 6) of the paper, the class of Moufang loops satisfying (1.1) is replaced by the (containing) class of Moufang loops satisfying the identical relation

$$(x\,y\,x)^2 = x^2\,y^2\,x^2. \tag{1.2}$$

As shown in Chapter VII, § 5 of [*1*], a subclass, namely those Moufang loops G for which the square-mapping is a semi-automorphism [that is, (1.2) holds and every element of G has a unique square-root in G] is intimately related in one manner (Chapter VII, Theorem 5.3) to the class of commutative Moufang loops and, in another manner (Chapter VII, Theorem 5.4) to the class of Moufang loops satisfying (1.1). The theory of this subclass could not be completed in [*1*] since it depended on the theory of commutative Moufang loops and, more specifically, on the material of § 5 of the present paper. Theorem 6.1 gives a fairly complete structural picture of this subclass.

In Theorems 6.2, 6.3, G is an arbitrary Moufang loop satisfying (1.2). *If F is the set of all periodic elements of G, F is a characteristic normal subloop of G and a direct product of its primary components $F(p)$* (Theorem 6.2). In addition, the structure of $F(p)$ is clarified for $p \geqq 3$ but not for $p = 2$. Moreover, if D is the intersection of the subloops G^n where n ranges over the odd integers, the structure of $H = G/D$ is given in Theorem 6.3. At this point, if we first divide out $F(2)$, so that G is a Moufang loop satisfying (1.2) in which each element has at most one square root, the main stumbling block in the way of describing the structure of G is the problem of "completing" G with respect to the square-root operation. We can indeed complete G (essentially uniquely) to a *di-associative* loop G^* which satisfies (1.2) and is closed under the square-root operation (Theorem 6.4); but we are unable to prove in general that G^* is Moufang. If it should be true that G^* is Moufang, then G^* would satisfy the hypothesis of Theorem 6.1 and the structure of G would be essentially known.

It seems worthwhile, in conclusion, briefly to summarize the state of the theory of Moufang loops. The structure of the Moufang loops (including the

commutative Moufang loops) which satisfy (1.1) is now relatively complete; and, to a lesser extent, the same is true of the Moufang loops satisfying (1.2). The isotopy-isomorphy problem for Moufang loops (in view of Theorems 1.1, 1.2) is well on its way toward solution and perhaps could be completed by a closer study of Moufang loops of exponent 3. Quite a little is known about central systems of a Moufang loop, but it is unknown whether the transfinitely continued descending central series of a free Moufang loop (or even of a free commutative Moufang loop) ends in the identity subloop. Practically nothing is known about simple Moufang loops other than groups (though a large class of simple non-associative Moufang loops has been exhibited by PAIGE [2]). And the Burnside problem for Moufang loops has essentially only been solved (Compare Theorems 5.2, 6.1) for exponent 3.

2. COMPANIONS. A one-to-one mapping ϑ of a loop G upon itself is a *pseudo-automorphism* of G provided there exists at least one element a of G, called a *companion* of ϑ, such that

$$[(x\,y)\,\vartheta]\,a = (x\,\vartheta)\,[(y\,\vartheta)\,a] \tag{2.1}$$

for all x, y in G. For any loop G the pseudo-automorphisms form a group. However, pseudo-automorphisms seem to occur naturally only in the study of restricted classes of loops, the most important class to date being that of the Moufang loops.

We shall assume henceforth that G is a Moufang loop with nucleus N. It will be convenient to list the following facts, each of which is either immediately obvious or proved explicitly in Chapter VII of [1]:

(i) *N is a normal subloop of G.*

(ii) *If a is a companion of a pseudo-automorphism ϑ of G, the coset $Na = aN$ is the set of all companions of ϑ.*

(iii) *If ϑ, φ are pseudo-automorphisms of G with companions a, b respectively, then $\vartheta\varphi$ has companion $(a\vartheta)b$ and ϑ^{-1} has companion $(a\vartheta^{-1})^{-1}$.*

(iv) *If ϑ is a pseudo-automorphism (or even a semi-endomorphism) of G, then*

$$x^n\,\vartheta = (x\,\vartheta)^n \tag{2.2}$$

for every x in G and every integer n.

(v) *$N\vartheta = N$ for every pseudo-automorphism ϑ of G.*

(vi) *Every inner mapping of G is a pseudo-automorphism of G. Companions for the generators of the inner mapping group are as follows (for all x, y in G):*

$$T(x) \quad \text{has companion} \quad x^{-3}; \tag{2.3}$$

$$R(x,y) = L(x^{-1}, y^{-1}) \quad \text{has companion} \quad (x,y) = x^{-1}y^{-1}xy. \tag{2.4}$$

It will be convenient to begin with the following lemma:

LEMMA 2.1. *Let the subloop H of the Moufang loop G have a generating subset B such that $B\vartheta < H$ for every pseudo-automorphism ϑ of G. Then H is a characteristic normal subloop of G and $H\vartheta = H$ for every pseudo-automorphism ϑ of G.*

PROOF. By (vi) above, $B\vartheta < H$ for every inner mapping ϑ of G. Hence, by Chapter IV, Lemma 1.4 of [1], H is a normal subloop of G. Now let K be the set of all k in H such that $k\vartheta$ is in H for every pseudo-automorphism ϑ of G. By hypothesis, $B < K$. By (2.2), $K^{-1} = K$. If k, k' are in K, (2.1) yields

$$[(k\,k')\,\vartheta]\,a \equiv a \bmod H$$

for every pseudo-automorphism ϑ with companion a. Hence $KK < K$. Therefore $K = H$. Since the pseudo-automorphisms form a group, $H\vartheta = H$ for every pseudo-automorphism ϑ. Since automorphisms are pseudo-automorphisms, H is characteristic. This completes the proof of Lemma 2.1.

The question remains open as to whether the pseudo-automorphisms of G induce pseudo-automorphisms of H. The answer is known to be affirmative when $H = N$.

For each integer n, let G^n denote the subloop generated by the n-th powers of the elements of the Moufang loop G. Then, by (2.2), (v) and Lemma 2.1, we have the following:

THEOREM 2.1. *Let G be a Moufang loop with nucleus N. Then, for every integer n, N, G^n and NG^n are characteristic normal subloops of G.*

We are now ready to study the companions of pseudo-automorphisms of G. We shall make use of the subloop NG^3 $(n = 3)$.

LEMMA 2.2. *Let G be a Moufang loop with nucleus N. Let $\mathfrak{P}$ be a group of pseudo-automorphisms of G which contains the inner mapping $T(x)$ of G for every x in G. Let C be the set of all companions of elements of $\mathfrak{P}$, and let M be the set of all m in G such that $mC < C$. Then*

(a) *m is in M if and only if $m\mathfrak{P} < C$;*

(b) *$NG^3 < M = M\mathfrak{P} < C$;*

(c) *M is a subloop of G;*

(d) *$C\,T(x) = C$ for every x in G.*

REMARK. Lemma 2.2 bears at least a superficial resemblance to Chapter VII, Lemma 3.4 of [1].

PROOF. (a) Let ϑ, a be elements of $\mathfrak{P}$, C, respectively, such that a is a companion of ϑ. Then, by (ii), ϑ^{-1} is in $\mathfrak{P}$ and has companion b where

$$(a\,\vartheta^{-1})\,b = 1.$$

First assume that m is in M. Then $m\,a$, as an element of C, is the companion of some φ in $\mathfrak{P}$. By (iii), $\varphi\vartheta^{-1}$ has companion

$$[(m\,a)\,\vartheta^{-1}]\,b = (m\,\vartheta^{-1})\,[(a\,\vartheta^{-1})\,b] = m\,\vartheta^{-1}.$$

Therefore $m\vartheta^{-1}$ is in C for each ϑ in $\mathfrak{P}$. That is, $m\mathfrak{P} < C$.

Next assume that m is an element of G such that $m\mathfrak{P} < C$. Then $m\vartheta^{-1}$ is in C and hence is a companion of some φ in $\mathfrak{P}$. Then $\varphi\vartheta$ has companion

$$[(m\,\vartheta^{-1})\,\vartheta]\,a = m\,a.$$

Hence $m\,a$ is in C for every a in C. That is, $mC < C$, m is in M. This proves (a).

(b) By (a), $M\mathfrak{P}\subset C$. Since $\mathfrak{P}$ is a group, $(M\mathfrak{P})\mathfrak{P}\subset M\mathfrak{P}\subset C$. Therefore, by (a) again, $M\mathfrak{P}\subset M$. And finally, since $\mathfrak{P}$ is a group, $M=M\mathfrak{P}\subset C$.

By (ii), $NC\subset C$. Therefore, by the definition of M, $N\subset M$.

By (vi), for each x in G, x^3 is a companion oj the element $T(x^{-1})$ of $\mathfrak{P}$. By this and (iv), $x^3\mathfrak{P}=(x\mathfrak{P})^3\subset C$. Therefore x^3 is in M for each x in G.

At this point it is clear that we may complete the proof of (b) by proving (c).

(c) If m is in M then m^{-3} is in M, since x^3 is in M for every x in G. Therefore

$$m^{-1}C=m[m(m^{-3}C)]\subset C,$$

whence we see that $M^{-1}=M$. In addition, if a is in C, so that $T(a)^{-1}$ is in $\mathfrak{P}$,

$$am=[mT(a)^{-1}]a\subset MC\subset C.$$

Hence $CM\subset C$. Finally, if m, m' are in M and c is in C, we use the Moufang identity $(xy)(zx)=x(yz)x$ to get

$$(mm')c=(mm')[(cm^{-1})m]=m[m'(cm^{-1})]m\subset C.$$

Therefore $MM\subset M$; and we conclude that M is a subloop of G. This proves (c) and completes the proof of (b).

(d) For each x in G, $\vartheta=T(x)$ is in $\mathfrak{P}$ and its companion $m=x^{-3}$ is in M. By (iii), C contains $C\vartheta\cdot m$. By part of the proof of (c), C also contains

$$(C\vartheta\cdot m)m^{-1}=C\vartheta.$$

Hence $C\vartheta\subset C$. Since $\vartheta^{-1}=T(x^{-1})$, we have proved (d) and completed the proof of Lemma 2.2.

THEOREM 2.2. *Let G be a Moufang loop with nucleus N and let $\mathfrak{T}$ be the group generated by the inner mappings $T(x)$, where x ranges over G. Then NG^3 is the set of all companions of elements of $\mathfrak{T}$.*

PROOF. By (vi), $\mathfrak{T}$ is a group of pseudo-automorphisms of G. We set $\mathfrak{P}=\mathfrak{T}$ and use the notation of Lemma 2.2. The hypotheses of the lemma apply. By (d) of the lemma, $C\mathfrak{P}=C$; hence, by (a) of the lemma, $M=C$. We wish, however, to prove that $NG^3=C$. To that end, we let $\mathfrak{Q}$ be the set of all elements of $\mathfrak{P}$ whose companions lie in NG^3. Since $(NG^3)\mathfrak{P}\subset NG^3$, it follows easily that $\mathfrak{Q}$ is a subgroup of $\mathfrak{P}$. Moreover, $\mathfrak{Q}$ contains $T(x)$ for every x, and therefore $\mathfrak{Q}=\mathfrak{P}$. Hence $C=NG^3$, completing the proof of Theorem 2.2.

3. SOME ISOTOPIC INVARIANTS. For our present purpose it will be necessary to draw together material from various parts of [*1*]. We shall do this as briefly as possible, consistent with clarity. In particular, a reference such as IV.1 or IV (3.7) refers to section 1 or equation (3.7) of Chapter IV of [*1*].

First we must refer to III.1. Isotopy is an equivalence relation. If a loop H is isotopic to a loop G, then H is isotopic to a principal isotope of G. If $(G,\bullet)$, $(G,\circ)$ are two loops with the same elements, (G,ϵ) is a principal isotope of $(G,\bullet)$ provided there exist elements a, b of G such that

$$(x\bullet a)\circ(b\bullet y)=x\bullet y \tag{3.1}$$

for all x, y of G. If the loop $(G, \bullet)$ is given, (3.1) defines a loop $(G, \circ)$. Moreover, $(G, \bullet)$ is a principal isotope of $(G, \circ)$:

$$(x \circ b) \bullet (a \circ y) = x \circ y \tag{3.2}$$

for all x, y in G.

From III.2 combined with the theory of normal subloops in IV. 1 we draw the following: If ϑ is a homomorphism of $(G, \bullet)$ upon a loop $(G\vartheta, \bullet)$, then ϑ is a homomorphism of $(G, \circ)$ upon a loop $(G\vartheta, \circ)$, and conversely. There exists a one-to-one inclusion-preserving mapping λ of the lattice $\mathfrak{N}$ of all normal subloops of $(G, \bullet)$ upon the lattice $\mathfrak{N}_0$ of all normal subloops of $(G, \circ)$. We may define λ and $\mu = \lambda^{-1}$ as follows:

$$P\lambda = b \bullet a \bullet P = b \bullet P \bullet a = P \bullet b \bullet a \quad \text{for } (P, \bullet) \text{ in } \mathfrak{N}; \tag{3.3}$$

$$Q\mu = a \circ b \circ Q = a \circ Q \circ b = Q \circ a \circ b \quad \text{for } (Q, \circ) \text{ in } \mathfrak{N}_0. \tag{3.4}$$

In each case, bracketing is unnecessary. The next result is not quite immediate: If $(H, \bullet)$, $(K, \bullet)$ are in $\mathfrak{N}$ and if $H \subset K$, then the quotient loop $(K/H, \bullet)$ lies in the centre (or left or right or middle nucleus) of $(G/H, \bullet)$ if and only if $(K\lambda/H\lambda, \circ)$ lies in the like-named subloop of $(G/H\lambda, \circ)$. This result may be obtained by combining III.2 (iii), III.2 (iv) with IV.1.

Next we wish to discuss nilpotency. We shall be especially interested in central nilpotency but it seems worthwhile to proceed with a little more generality. First consider VI.1 and let $\mathfrak{L}$ be a class of loops satisfying the conditions (a), (b) there stated and the additional condition

(c) *If G is in $\mathfrak{L}$, every loop isotopic to G is in $\mathfrak{L}$.*

Next let f be a nilpotency function for $\mathfrak{L}$ which satisfies, in addition to the conditions (i)—(iv) of IV.1, the condition

(v) *For each G in $\mathfrak{L}$, $f(G)$ is a subloop of some specified one (or of the intersection of some specified ones) of the centre, left nucleus, right nucleus or middle nucleus of G.*

We wish to state one result covering the lower (descending) and upper (ascending) f-series discussed in VI.1 and the other possible varieties of f-systems discussed in VI.4. We may do this most effectively by reference to the *order-type* of an f-system ,since the order-type specifies not only whether the f-series is ascending (for example) but also its "length". Then, from the remarks two paragraphs above, we may state the following theorem for any class $\mathfrak{L}$ of loops satisfying (a), (b), (c) of the preceding paragraph and for any nilpotency function f of $\mathfrak{L}$ satisfying (i)—(v):

If G is in $\mathfrak{L}$ and if G has an f-system of a specified order-type, then every loop isotopic to G is in $\mathfrak{L}$ and has an f-system of the same order-type.

At this point we specialize to the case of central nilpotency. Then $\mathfrak{L}$ is the class of all loops and $f(G)$ is the centre of G. We state the result as a formal theorem:

THEOREM 3.1. *If a loop G has a central system of a given order-type, then every loop isotopic to G has a central system of the same order-type.*

Next we wish to consider subloops of the principal isotopes $(G, \bullet)$, $(G, \circ)$. The following simple lemma will be convenient:

LEMMA 3.1. *Let the loops $(G, \bullet)$, $(G, \circ)$ be principal isotopes linked by* (3.1), (3.2), *and let S be any subset of G which contains the elements a, b. If S generates the subloop $(H, \bullet)$ of $(G, \bullet)$ and the subloop $(K, \circ)$ of $(G, \circ)$, then $K = H$ and the loops $(H, \bullet)$, $(H, \circ)$ are principal isotopes linked by* (3.1), (3.2).

REMARK. Examples show that each of the following possibilities can occur if S does not contain a, b: (i) $K \neq H$ and $(H, \circ)$ is not even a subloop of $(G, \circ)$; (ii) $(H, \circ)$ is a subloop of $(G, \circ)$ but $(H, \circ)$ is not an isotope (let alone a principal isotope) of $(H, \bullet)$.

PROOF. The set H contains S and therefore a, b. Therefore (3.1), with x, y restricted to H, defines a subloop $(H, \circ)$ of $(G, \circ)$; and $(H, \circ)$ is a principal isotope of $(H, \bullet)$. Since $(H, \circ)$ is a subloop of $(G, \circ)$ containing S, and since S generates $(K, \circ)$, then $K < H$. Similarly, by use of (3.2), $H < K$. Therefore $K = H$ and the proof of Lemma 3.1 is complete.

We recall that a loop G is said to have a property P *locally* if every finitely generated subloop of G has P. The following theorem tells us that certain properties are isotopic invariants:

THEOREM 3.2. *If G is a loop having one of the following properties, then every loop isotopic to G has the same property:*

(i) *G is finite.*

(ii) *G is locally finite.*

(iii) *G is centrally nilpotent (i.e., of finite class).*

(iv) *G is locally centrally nilpotent.*

PROOF. We need only consider a pair of principal isotopes $(G, \bullet)$, $(G, \circ)$, linked by (3.1), (3.2). If $(G, \bullet)$ has property (i) then (trivially) so has $(G, \circ)$. If $(G, \bullet)$ has (iii) then, by Theorem 3.1, so has $(G, \circ)$. Moreover, each of (i), (iii) is inherited by subloops. If $(G, \bullet)$ has property (ii) (or (iv)) and if $(M, \circ)$ is a subloop of $(G, \circ)$ generated by a finite subset T, we let S be T with a, b adjoined. If S generates $(H, \bullet)$ then, $(H, \bullet)$ has property (i) [or (iii)]. By Lemma 3.1, S also generates $(H, \circ)$, a principal isotope of $(H, \bullet)$, and, by the first part of the proof, $(H, \circ)$ has property (i) [or (iii)]. Also $(M, \circ)$, as a subloop of $(H, \circ)$, has property (i) [or (iii)]. Therefore $(G, \circ)$ has property (ii) [or (iv)]. This completes the proof of Theorem 3.2.

4. SOME FINITENESS PROPERTIES. In the following we shall adapt some known theorems for groups to loops satisfying certain properties. Let G be a loop, $Z(G)$ be the centre of G and G' be the commutator-associator subloop of G. We recall that any subloop of $Z(G)$ is automatically normal in G.

LEMMA 4.1. *If A is a subloop of the loop G such that* (a) *$A < Z(G)$ and* (b) *G/A is finite, then*

(i) *G' is finitely generated;*

(ii) *A is finitely generated if G is.*

PROOF. (i) Since G/A is finite and $A<Z(G)$, then $G/Z(G)$ is finite. We know that G' is generated by the set of all commutators (x, y) and associators (x, y, z) where x, y, z range over G. However, $(xa, yb)=(x, y)$ and $(xa, yb, zc)=(x, y, z)$ for all x, y, z in G and a, b, c in $Z(G)$. Hence, since $G/Z(G)$ is finite, G' is finitely generated.

(ii) By the axiom of choice, there exists at least one single-valued function f from G into G such that

$$x A = f(x) A, \qquad \text{all } x \text{ in } G; \tag{4.1}$$

$$f(x a) = f(x), \qquad \text{all } x \text{ in } G,\ a \text{ in } A. \tag{4.2}$$

Taking $x=1$ in (4.2), we see that

$$f(a) = f(1), \qquad \text{all } a \text{ in } A. \tag{4.3}$$

Fixing attention on one such f, we define a function g by

$$x = f(x)\, g(x), \quad \text{all } x \text{ in } G. \tag{4.4}$$

By (4.1), $g(x)$ is in A for every x in G.

By (4.1), (4.2) and the fact G/A is finite, the set $f(G)$, consisting of the elements $f(x)$ as x ranges over G, is finite. Hence the set R, consisting of the elements $g\big(f(x)\, f(y)\big)$, where x, y range over G, is finite also.

Now let S be a generating subset of G. The set $g(S)$, consisting of the elements $g(s)$ as s ranges over S, will be finite if S is finite. Hence we shall prove (ii) by proving that $R \cup g(S)$ generates A.

By construction, $R \cup g(S)$ is a subset of A and hence generates a subloop B of A. Since $B<A<Z(G)$, B is normal in G.

Let H be the set of all h in G such that $h \equiv f(h) \bmod B$. Since B contains $g(S)$, we see from (4.4) that S is in H. Next let x, y, z be elements of G such that $xy=z$. Then, certainly,

$$x y \equiv z \mod B. \tag{4.5}$$

In addition, $f(z)A = zA = xA \cdot yA = f(x)A \cdot f(y)A = f(x)f(y) \cdot A$, by (4.1), and hence

$$f(x)\, f(y) = f(z)\, g\big(f(x)\, f(y)\big)$$

by (4.2). Therefore, since B contains R,

$$f(x)\, f(y) \equiv f(z) \mod B. \tag{4.6}$$

By comparison of (4.5), (4.6) we see that if any two of the congruences

$$x \equiv f(x), \qquad y \equiv f(y), \qquad z \equiv f(z) \mod B$$

are valid, the third is valid also. Consequently, H is a subloop of G. Since H contains S, we conclude that $H=G$. That is,

$$x \equiv f(x) \mod B, \quad \text{all } x \text{ in } G. \tag{4.7}$$

Since 1 is in B, we see from (4.7) that $f(1)$ is in B. Therefore, by (4.3), (4.7), $A<B$. However, $B<A$ by construction, so $A=B$. That is, $R \cup g(S)$ generates A. This proves (ii) and completes the proof of Lemma 4.1.

The author does not know whether the following statement is true or false: *If N is a normal subloop of finite index in a finitely generated loop G, then N is finitely generated.* The corresponding statement for groups is, of course, well known to be true.

Next we recall that a loop G is *di-associative* if every two elements of G generate a group.

LEMMA 4.2. *Let G be a di-associative loop containing a subloop A such that* (a) $A \subset Z(G)$ *and* (b) G/A *is finite. Let the integer m be divisible by the least common multiple of the orders of the subloops of G/A which can be generated by two elements. Then the power-mapping* (m): $x \to x^m$, *is an endomorphism of G into A.*

PROOF. Let x, y be any two elements of G (not necessarily distinct) and consider the subloop H of G which is generated by x, y. The hypothesis of di-associativity tells us that H is a group. Then $H/(H \cap A)$, as an isomorph of the subloop HA/A of G/A, has finite order, say e. Since HA/A can be generated by two elements, e is a divisor of m. Since $A \subset Z(G)$, then $H \cap A \subset H \cap Z(G) \subset Z(H)$. To sum up, H is a group, $H \cap A$ is part of $Z(H)$, and $H/(H \cap A)$ has finite order e. Therefore, by a known theorem on groups, the mapping $h \to h^e$ is an endomorphism of H into $H \cap A$. A fortiori, since e divides m, the mapping $h \to h^m$ is an endomorphism of H into A. In particular, $(xy)^m = x^m y^m$ and x^m is in A. Since x, y were arbitrary elements of G, the proof of Lemma 4.2 is complete.

THEOREM 4.1. *If G is a di-associative loop and if $G/Z(G)$ is finite, then G' is finite also.*

PROOF. By Lemma 4.1(i), G' is finitely generated. By Lemma 4.2, there exists a positive integer m such that the power mapping (m): $x \to x^m$, is an endomorphism of G into $Z(G)$. Since $Z(G)$ is an abelian group, $G'(m) = 1$; that is, G' has exponent dividing m. Since $G'/(G' \cap Z(G))$ is isomorphic to the subloop $G'Z(G)/Z(G)$ of the finite loop $G/Z(G)$, then $G'/(G' \cap Z(G))$ is finite. Hence, by Lemma 4.1(ii), since $G' \cap Z(G) \subset Z(G')$, then $G' \cap Z(G)$ is finitely generated. Therefore $G' \cap Z(G)$, being a finitely generated abelian group of exponent dividing m, is finite. And since $G'/(G' \cap Z(G))$ and $G' \cap Z(G)$ are both finite, G' must be finite also. This proves Theorem 4.1.

THEOREM 4.2. *If G is a di-associative loop and if $G/Z(G)$ is locally finite, then G' is locally finite also.*

PROOF. If K is a finitely generated subloop of G', there exists a finitely generated subloop H of G such that $K \subset H'$. Then $HZ(G)/Z(G)$, being a finitely generated subloop of the locally finite loop $G/Z(G)$, is finite. Therefore $H/(H \cap Z(G))$ is finite and, since $H \cap Z(G) \subset Z(H)$, we conclude that $H/Z(H)$ is finite. Hence, by Theorem 4.1, H' is finite. Since $K \subset H'$, we see that K is finite also. That is, G' is locally finite. This proves Theorem 4.2.

THEOREM 4.3. *If G is a di-associative loop and if $G/Z(G)$ is locally finite, then the subset P of G, consisting of all elements of G of finite order, is a locally finite characteristic normal subloop of G. Moreover, G/P is an abelian group.*

PROOF. Let H be a subloop of G generated by a finite set of elements of finite order. Just as in the proof of Theorem 4.2, H' is finite. In addition, H/H', being an abelian group generated by finitely many elements of finite order, is finite. Hence H is finite. This shows both that P is a subloop of G and that P is locally finite. Obviously P is characteristic. Since, by Theorem 4.2, P contains G', then P is normal in G and G/P is an abelian group. This proves Theorem 4.3.

5. A CLASS OF MOUFANG LOOPS. We propose to study the class of all Moufang loops G which satisfy the identity

$$(x\,y)^3 = x^3\,y^3 \tag{5.1}$$

for all x, y in G. We begin with a curious lemma which does not seem to be widely known even for groups:

LEMMA 5.1. *If G is a Moufang loop in which* (5.1) *holds identically, then the mapping $x \to x^3$ is a centralizing endomorphism of G.*

PROOF. For any integer n, let (n) denote the power-mapping defined by

$$x(n) = x^n \tag{5.2}$$

for every x in G. We shall first prove Lemma 5.1 on the assumption that G is a group.

By hypothesis, (3) is an endomorphism (and hence a normal endomorphism) of G. Since the complement of a normal endomorphism is also an endomorphism (-2) is an endomorphism of G. But then $(-2)^2 = (4)$ and its complement, (-3), are endomorphisms of G. Since (3) and (-3) are endomorphisms, $G(3)$ must be commutative. At this stage we need the definition of the commutator (x, y):

$$x\,y = [y\,x]\,(x, y) \tag{5.3}$$

for all x, y in G. The fact that (3) is a normal endomorphism implies that

$$(x, y)^3 = (x^3, y) = (x, y^3) \tag{5.4}$$

for all x, y in G. Hence, since $G(3)$ is commutative,

$$(x^3, y) = 1 \tag{5.5}$$

for all x, y in G.

When G is a group, (5.5) implies that x^3 lies in the centre of G for each x in G; and this is what we set out to prove. When G is merely a Moufang loop we use the results of [3]. If we replace "normal" by "semi-normal", every sentence in the preceding paragraph remains valid. Moreover, if we define the associator (x, y, z) by

$$(x\,y)\,z = [x(y\,z)]\,(x, y, z) \tag{5.6}$$

for all x, y, z in G, the fact that (3) is semi-normal implies that

$$(x, y, z)^3 = (x^3, y, z) = (x, y^3, z) = (x, y, z^3) \tag{5.7}$$

for all x, y, z in G. We know that $G(3)$ is a commutative Moufang loop. If K is a commutative Moufang loop then (by Chapter VII, Lemma 5.7 of [1]) k^3 lies in the centre of K (an abelian group) for every k in K. Hence $(3)^2$ maps G into an abelian group; and, of course, $(3)^3$ does so also. Therefore, from (5.7),

$$(x, y, z)^3 = (x^3, y^3, z^3) = (x, y, z)^{27} = 1$$

and hence

$$(x^3, y, z) = (x, y^3, z) = (x, y, z^3) = 1 \tag{5.8}$$

for all x, y, z in G. In view of (5.5), (5.8), x^3 lies in the centre of G for every x in G. This completes the proof of Lemma 5.1.

By combining Lemma 5.1 with Chapter VII, Theorem 5.5 of [1], we get the following:

THEOREM 5.1. *Let G be a Moufang loop. A necessary and sufficient condition that G satisfy the identical relation* (5.1) *is that G be either an isotope of a commutative Moufang loop or a normal subloop of index three in such a loop-isotope.*

It is now quite easy to verify that the class of all Moufang loops satisfying the identical relation (5.1) contains the subloops, the homomorphic images and the loop-isotope of its members. In addition, we are now in a position to carry over to this class of loops a variety of theorems on commutative Moufang loops. Our results will be embodied in a single theorem.

THEOREM 5.2. *Let G be a Moufang loop which satisfies the identical relation* (5.1). *Then, if G has centre $Z = Z(G)$, commutator-associator subloop G', inner mapping group $\mathfrak{I} = \mathfrak{I}(G)$, multiplication group $\mathfrak{M} = \mathfrak{M}(G)$, the following statements are true:*

(i) *G is locally centrally nilpotent.*

(ii) *Every composition chief system of G is a central system of G.*

(iii) *G' and G/Z are locally finite loops of exponent 3, and are finite if G is finitely generated.*

(iv) *The set P of all elements of G of finite order is a locally finite characteristic normal subloop of G, and G/P is an abelian group.*

(v) *$\mathfrak{I}$, $\mathfrak{M}'$ and $\mathfrak{M}/Z(\mathfrak{M})$ are locally finite 3-groups, and are finite if G is finitely generated.*

COROLLARY 1. *The simple Moufang loops satisfying the identical relation* (5.1) *are the group of order one and the cyclic groups of prime order.*

COROLLARY 2. *If $G \neq 1$ is a simple Moufang loop and if $G^3 = 1$, then G is a cyclic group of order three.*

PROOF. By Theorem 5.1, if G is a Moufang loop satisfying the identical relation (5.1), there exists a commutative Moufang loop C and a loop H isotopic to C such that either $G = H$ or G is a normal subloop of index 3 in H. Of course, H is a Moufang loop satisfying the identical relation (5.1). Since the properties to be proved are preserved under isomorphism, we may and do assume that H is a principal isotope of C. Indeed, by Chapter VII, Lemma 5.8 of [1], we may assume that H is the principal isotope $(C, \circ)$ of

$C=(C, \circ)$ given by

$$x \circ y = (xf)(f^{-1}y) \tag{5.9}$$

where f is some fixed element of C and where x, y range over C. We now treat (i)–(v) in turn.

(i) By Chapter VIII, Theorem 10.1 of [1], C is locally centrally nilpotent. By Theorem 3.2, H is locally centrally nilpotent. Therefore G is locally centrally nilpotent. This proves (i).

(ii) Every homomorphic image of G is a Moufang loop satisfying the identical relation (5.1) and hence, by (i), is locally centrally nilpotent. In particular, then, every homomorphic image of G is a local Z-loop. Consequently, as pointed out in the first part of the proof of Chapter VI, Theorem 4.1 of [1], every composition chief system of G is a central system. This proves (ii).

(iii) By Chapter VIII, Theorem 11.4 of [1], $C/Z(C)$ is locally finite. Also, as a consequence of the discussion in § 3, $H/Z(H)$ is isotopic to $C/Z(C)$. Hence, by Theorem 3.2, $H/Z(H)$ is locally finite. Since $GZ(H)/Z(H)$ is a subloop of $H/Z(H)$ and is isomorphic to $G/(G\cap Z(H))$, the latter is locally finite. Since $G\cap Z(H)<Z(G)$, then $G/Z(G)$ is a homomorphic image of a locally finite loop and hence is locally finite.

Since $G/Z(G)$ is locally finite, we see from Theorem 4.2 that G' is locally finite.

If G is finitely generated, so is $G/Z(G)$. But then $G/Z(G)$ is finite and hence, by Theorem 4.1, G' is finite also. This proves (iii).

(iv) Since $G/Z(G)$ is locally finite, (iv) follows from Theorem 4.3.

(v) By Chapter VIII, Theorem 11.4 of [1], $\mathfrak{J}(C)$, $\mathfrak{M}(C)'$ and $\mathfrak{M}(C)/Z(\mathfrak{M}(C))$ are locally finite 3-groups and are finite if C is finitely generated. Assuming that H is given by (5.9), we verify easily that $\mathfrak{M}(H)=\mathfrak{M}(C)$, $\mathfrak{J}(H)=\mathfrak{J}(C)$. Moreover, if H is finitely generated, then, by Lemma 3.1, C is finitely generated also. This proves (v) for the case that $G=H$.

Now let us assume that G is a normal subloop of index 3 in H. If h is in H but not in G, then h and G generate H; in particular, H is finitely generated if G is. Let $\mathfrak{N}$ be the subloop of $\mathfrak{M}(H)$ generated by the set of all right and left multiplication of H corresponding to elements of G; and let $\mathfrak{K}=\mathfrak{N}\cap\mathfrak{J}(H)$. Then $\mathfrak{N}$ and $\mathfrak{K}$ induce $\mathfrak{M}=\mathfrak{M}(G)$ and $\mathfrak{J}=\mathfrak{J}(G)$, respectively, on G. Certainly $\mathfrak{N}'$ and $\mathfrak{K}$ are locally finite 3-groups; hence $\mathfrak{M}'$ and $\mathfrak{J}$ are, also. If $\mathfrak{P}$ is the subgroup of $\mathfrak{N}$ which induces $Z(\mathfrak{M})$ on G, then, obviously, $\mathfrak{N}\cap Z(\mathfrak{M}(H))<\mathfrak{P}$. Since $\mathfrak{M}(H)/Z(\mathfrak{M}(H))$ is a locally finite 3-group, we see easily that $\mathfrak{N}/\mathfrak{P}$ and $\mathfrak{M}/Z(\mathfrak{M})$ are locally finite 3-groups too. Finally, if G is finitely generated, then H is finitely generated and, a fortiori, each of $\mathfrak{J}$, $\mathfrak{M}'$, $\mathfrak{M}/Z(\mathfrak{M})$ is finite. This proves (v) and completes the proof of Theorem 5.2.

Corollary 1 follows from the fact a simple loop which possesses a central system is necessarily an abelian group and hence, as a simple abelian group, is either a group of order one or a cyclic group of prime order. On the other hand, every abelian group satisfies the identity (5.1). Corollary 2 is a direct consequence of Corollary 1.

6. ANOTHER CLASS. By SVII Lemma 5.2, the class of Moufang loops G satisfying the identity (5.1) is included in the class satisfying

$$(x\,y\,x)^2 = x^2\,y^2\,x^2. \tag{6.1}$$

By SVII Lemma 5.1, the identity (6.1) is equivalent for a Moufang loop G to each of the identities

$$\big((x,\,y),\,y\big) = 1\,, \tag{6.2}$$

$$(x,\,y)^n = (x^n,\,y) = (x,\,y^n)\,, \tag{6.3}$$

$$(x\,y)^n = x^n\,y^n\,(x,\,y)^{-n\,(n-1)/2}, \tag{6.4}$$

$$(x\,y\,x)^n = x^n\,y^n\,x^n, \tag{6.5}$$

the last three being understood to hold for all integers n.

The identity (6.5) states that the power-mapping (n) is a *semi-endomorphism* of G. If (n) were also one-to-one upon G, we would call (n) a *semi-automorphism* of G. In SVII.5 we studied the case that the square-mapping (2) was a semi-automorphism. Here we wish to broaden and sharpen the earlier results.

As in SVII.5, the mapping $P(x)$ of the Moufang loop G is defined by

$$P(x) = L(x)\,R(x) = R(x)\,L(x) \tag{6.6}$$

for each x in G. By SVII Lemma 5.8, every loop isotopic to a Moufang loop $G = (G, \bullet)$ is isomorphic to some principal isotope $(G, \circ)$ of type (5.9). If x is in G, the powers of x are the same in $(G, \circ)$ as in $(G, \bullet)$. Moreover, by the standard Moufang identities (see SVII Lemma 3.1),

$$x \circ y \circ x = (x\,f)\,\{f^{-1}\,[(y\,f)\,(f^{-1}\,x)]\} = (x\,f)\,[(f^{-1}\,y)\,x] = x\,y\,x\,,$$

for all x, y in G. In particular, we deduce the following:

The class of all Moufang loops satisfying the identity (6.1) *contains the loop-isotopes of each of its members.*

In addition we see that, for a Moufang loop G, *any property of the mappings* $P(x)$ *which is preserved under isomorphism is also preserved under loop-isotopy.* This prepares us for the following lemma:

LEMMA 6.1. *Let G be a Moufang loop. The equation*

$$P(x)\,P(y) = P(y)\,P(x) \tag{6.7}$$

holds for all x, y in G if and only if G satisfies the following two conditions:

(i) *Every commutator (x, y) lies in the nucleus N of G.*

(ii) $\big((x, y), z\big) = (x, y, z)^2$ *for all x, y, z of G.*

The conditions (i), (ii) *imply the following:*

(iii) *G satisfies the equivalent identities* (6.1)–(6.5).

(iv) *Every commutator (x, y) and associator (x, y, z) lies in the centre C of N. Hence the commutator-associator subloop G' is an abelian group.*

(v) *$(x, y, z)^2$ lies in the centre Z of G for all x, y, z in G.*

(vi) *G is centrally nilpotent of class at most 3.*

COROLLARY. *If* (i), (ii) *hold for a Moufang loop* G *such that either* $G=G^2$ *or* G *has no elements of order* 2, *then every associator* (x, y, z) *lies in the centre* Z *of* G.

REMARK. Lemma 6.1 is closely allied to SVII Lemma 5.6. The significant difference is that the square-mapping is not assumed to be a permutation of G; consequently, G may perhaps have elements of order 2 or elements which are not squares.

PROOF. *Sufficiency.* We assume (i), (ii) and deduce (6.7). First we note that (i), (ii) are the conditions (a), (c), respectively, of SVII Lemma 5.6. Moreover, (i) implies the equivalent identities of SVII Lemma 5.5 and hence implies, in particular, that each associator (x, y, z) lies in the centre of the subloop generated by its arguments x, y, z. This is enough to assure us that the calculations in the sufficiency proof of SVII Lemma 5.6 are valid under the assumption of (i), (ii). Hence (i), (ii) imply (6.7).

Necessity. We assume (6.7) and use the necessity proof of SVII Lemma 5.6 down to the point where we have deduced both (a) and (c), which are the present (i), (ii). Thus (6.7) implies (i) and (ii).

From this point on we use (i), (ii). From (ii) with $z=y$, we see that (6.2) holds identically. Hence (iii) is true by SVII Lemma 5.1. By combining (i) with the special case of (ii) in which z is in N, we see that every commutator (x, y) is in C. In view of (i), all the identities of SVII Lemma 5.1 are available. In particular, by SVII (5.21), SVII (5.22),

$$(x, y, z) = (y, x, z)^{-1} = (z, y, x)^{-1} \tag{6.8}$$

for all x, y, z in G. By (ii) and (6.8),

$$\big((x, z), y\big) = (x, z, y)^2 = (x, y, z)^{-2}.$$

Since, in addition, (x, y, z) lies in the centre of the subloop generated by x, y, z, SVII (5.23) may be replaced by the identity

$$(x\,y, z) = (x, z)\,(y, z)\,(x, y, z). \tag{6.9}$$

In as much as the commutators in (6.9) are elements of the subloop C, the same must be true of (x, y, z). This proves (iv).

We recall that N is a normal subloop of G. By (ii) we have

$$\big((n, y), z\big) = 1 \tag{6.10}$$

for all n in N and y, z in G. Since N is normal, (n, y) is in N and hence, by (6.10), (n, y) is in the centre $Z=Z_1$ of G, for all n in N, y in G. As one consequence, by (iv) and (ii), $\big((x, y), z\big) = (x, y, z)^2$ is in Z for all x, y, z in G. This proves (v). In addition, N is part of the second centre Z_2 of G. Hence, in view of (iv), G/Z_2 is an abelian group and thus $G=Z_3$. This means that G is centrally nilpotent of class at most 3. Hence (vi) holds and the proof of Lemma 6.1 is complete.

To prove the Corollary, we set $a=(x, y, z)$. Then, by (iv), a is in N. Also, by (v) and (6.3),

$$1=(a^2, w)=(a, w^2)=(a, w)^2$$

for every w in G. Since a is in N, the fact that $(a, w^2)=1$ for all w tells us that a commutes with every element of G^2. Hence a is in Z if $G=G^2$. On the other hand, if G has no elements of order 2, the fact that $(a, w)^2=1$ tells us that a is in Z. This proves the Corollary.

For an example of a Moufang loop G which satisfies (6.7) and is centrally nilpotent of class 3, see SVII Example 3. The example shows in particular that G need not have elements of finite order, aside from the identity element.

THEOREM 6.1. *Let the square-mapping* (2) *be a semi-automorphism of the Moufang loop G. Then:*

(i) *G_3 and G/Z_3 have exponent 3.*

(ii) *G^3 is centrally nilpotent of class at most 3.*

(iii) *The cube-mapping* (3) *induces centralizing endomorphisms of G' and G/Z_2. As a consequence, G is locally nilpotent. Hence, in addition, every composition chief system of G is a central system of G.*

COROLLARY. *If, in addition to the hypothesis of Theorem* 6.1, *G has no elements of order 3, then G satisfies the conditions* (i), (ii) *of Lemma* 6.1.

REMARK. Theorem 6.1 represents a sharpening of SVII Theorem 5.4.

PROOF. Let T be the set of all elements t of G such that $t^3=1$. Then, as in the proof of SVII Theorem 5.4, we verify that T is a normal subloop of G, that (2) induces a semi-automorphism of $H=G/T$, and that the loop $H(1/2)$ is an abelian group. As shown in the proof of SVII Lemma 5.6, the last statement means that (6.7) holds for all x, y in H. (Here we observe that the case $T=1$ yields the Corollary to Theorem 6.1.) To continue, we may assume that H satisfies (i)—(vi) of Lemma 6.1 and also the conclusion of the Corollary to Lemma 6.1. Thus we have

$$((x, y), z) \equiv (x, y, z)^2 \mod T \tag{6.11}$$

for all x, y, z in G, and

$$(c, x, y) \equiv (a, x, y) \equiv (a, x) \equiv 1 \mod T \tag{6.12}$$

for every commutator c, every associator a of G and all x, y in G. Moreover, by Lemma 6.1 (iv), H' is an abelian group. Equivalently,

$$G'/(G' \cap T) \text{ is an abelian group.} \tag{6.13}$$

In addition we may show, as in the proof of SVII Theorem 5.4, that

$$(x^3, y, z)=(x, y, z)^3 \tag{6.14}$$

for all x, y, z in G.

To see that G_3 has exponent 3 we need only recall that $H_3=1$ and hence $G_3 \subset T$. This proves the first part of (i).

Now suppose that u, v, w are in the commutator-associator subloop G'. Then, by (6.13),

$$(u, v) \equiv (u, v, w) \equiv 1 \mod T$$

and hence, by (6.3), (6.14)

$$(u^3, v) = (u^3, v, w) = 1.$$

Therefore $(G')^3$ is part of the centre of G'. Thence, by (6.4), (6.3),

$$(uv)^3 = u^3 v^3 (u^3, v)^{-1} = u^3 v^3,$$

so (3) induces a (centralizing) endomorphism of G'. This proves the first part of (iii).

If c is any commutator and a is any associator of G, we find from (6.12) together with (6.3), (6.14) that

$$(c^3, x, y) = (a^3, x, y) = (a^3, x) = 1$$

for all x, y in G. Thus

$$(x, y)^3 \equiv 1 \mod N, \qquad (x, y, z)^3 \equiv 1 \mod Z \tag{6.15}$$

for all x, y, z in G, where N is the nucleus and Z is the centre of G. If $c = (x, y)$, $a = (x, y, z)$, then, by (6.11), $(c, z) = a^2 t$ for t in T. Therefore, by (6.3), (6.4), (6.3)

$$(c^3, z) = (a^2 t)^3 = a^6 t^3 (a^2, t)^{-3} = a^6 (a^2, t^{-3}) = a^6.$$

Combining this with (6.15), we get

$$(x, y)^3 \equiv (x, y, z)^3 \equiv 1 \mod Z_2 \tag{6.16}$$

for all x, y, z in G, where Z_2 is the second centre of G. As in the case of G', we deduce from (6.16) that (3) induces a centralizing endomorphism of G/Z_2. This completes the proof of (iii). Next, (6.16), combined with (6.3), (6.14), yields

$$x^3 \equiv 1 \mod Z_3 \tag{6.17}$$

for every x in G, where Z_3 is the third centre of G. From (6.17) or from (ii) we deduce that G/Z_3 has exponent 3, completing the proof of (i). From (6.17) again, $G^3 < Z_3$. If $K = G^3$, the relation $K < Z_3$ implies successively that $K_1 < Z_2$, $K_2 < Z$, $K_3 = 1$. Hence G^3 is centrally nilpotent of class at most 3. This proves (ii).

By (iii), G/Z_2 satisfies the identity (5.1). Hence, as a consequence of Theorem 5.2, G/Z_2 is locally centrally nilpotent. If F is a subloop of G with second centre $Z_2(F)$, then $F \cap Z_2 < Z_2(F)$. Hence $F/Z_2(F)$ is a homomorphic image of $F/(F \cap Z_2)$, and the latter is isomorphic to the subloop FZ_2/Z_2 of G/Z_2. Therefore $F/Z_2(F)$ also satisfies (5.1) and hence is centrally nilpotent if F is finitely generated. In this case, F must be centrally nilpotent also. Thus we see that G is locally centrally nilpotent. Any homomorphic loop-image of a locally centrally nilpotent loop clearly has the same property. Therefore, by the first part of the proof of SVI Theorem 4.1, every composition chief system of G is a central system of G. This completes the proof of Theorem 6.1 and Corollary.

The question remains open as to whether Theorem 6.1 is still true when the word "semi-automorphism" in its hypothesis is replaced by "semi-endomorphism". We shall obtain some partial results in this direction.

THEOREM 6.2. *Let G be a Moufang loop in which* (6.1) *holds identically. Let F be the set of all elements of G of finite order and, for each prime p, let $F(p)$ be the set of all elements of G of order a power of p. Then:*

(i) *F and the primary components $F(p)$ are characteristic normal subloops of G, and F is a direct product of the $F(p)$.*

(ii) *If $p > 3$, $F(p)$ is centrally nilpotent of class at most 3 and $F(p)'$ is an abelian group.*

(iii) *$F(3)$ is locally centrally nilpotent, $F(3)_3$ has exponent 3, $F(3)^3$ is centrally nilpotent of class at most 3, and the cube-mapping* (3) *induces centralizing endomorphisms of $F(3)'$ and $F(3)/Z_2(F(3))$.*

PROOF. (i) Let n be the least common multiple of the orders of two elements x, y of F. Then $(x^{-1})^n = 1$ and $(x\,\vartheta)^n = (x^n)\vartheta = 1$ for any inner mapping ϑ of G. By (6.4), (6.3), where $s = 2n - 1$,

$$(x\,y)^{2n} = x^{2n}\,y^{2n}\,(x, y)^{-ns} = (x^n, y)^{-s} = 1.$$

Furthermore, if $n = 2k+1$ is odd,

$$(x\,y)^n = x^n\,y^n\,(x, y)^{-nk} = (x^n, y)^{-k} = 1.$$

This proves that F and the $F(p)$ are characteristic normal subloops of G. As an immediate consequence, F is a direct product of the $F(p)$, proving (i).

(ii), (iii). If $p \geqq 3$, every element of $F(p)$ is uniquely expressible as a square. Hence Theorem 6.1 applies and we get the conclusions of (ii) or (iii) according as $p > 3$ or $p = 3$.

This completes the proof of Theorem 6.2. Note that we have said nothing about the structure of the subloop $F(2)$.

THEOREM 6.3. *Let G be a Moufang loop in which* (6.1) *holds identically, and let D be the intersection of the subloops G^n as n ranges over all odd positive integers. Then the loop $H = G/D$ has the following properties:*

(i) *H is locally centrally nilpotent, H_3 and $H/Z_3(H)$ have exponent 3, H^3 is centrally nilpotent of class at most 3, and the cube-mapping* (3) *induces centralizing endomorphisms of H' and $H/Z_2(H)$.*

(ii) *If G has no elements of order 3 then H is centrally nilpotent of class at most 3 and H' is an abelian group. Indeed, H satisfies the conditions* (i), (ii) *of Lemma* 6.1 *and has no elements of order* 2.

PROOF. (i) If n is an odd positive integer, the loop G/G^n satisfies the hypothesis of Theorem 6.1. Hence H is isomorphic to a subdirect product of loops in which the conclusions of Theorem 6.1 are valid. All of these conclusions carry over to H, proving (i).

(ii) We begin by noting that if n is odd integer and if x, y are in G, then, by (6.4), (6.2), (6.3), (6.4), with $k = (n-1)/2$, $s = -k^2 n$,

$$[x\,y\,(x, y)^k]^n = (x\,y)^n\,(x, y)^{kn}\,\big(x\,y, (x, y)\big)^s = (x\,y)^n\,(x, y)^{kn} = x^n\,y^n.$$

Hence every element of G^n is an n-th power. Now assume that G has no element of order 3 and let x be an element of G such that x^3 is in G^{3n}. Then $x^3 = y^3$ where y is in G^n. However,

$$(x\,y^{-1})^3 = x^3\,y^{-3}(x, y^{-1})^{-3} = (x, y^3) = 1$$

and hence $x = y$. Thus the elements of order 3 in G/G^{3n} are all contained in G^n/G^{3n}. Therefore, as in the proof of Theorem 6.1, with G^n/G^{3n} taking the rôle of T, we may conclude that G/G^n satisfies the identity (6.7) of Lemma 6.1. Since this is true for each odd n, H must satisfy (6.7) and the equivalent conditions (i), (ii) of Lemma 6.1. Obviously H has no elements of order 2 (or, indeed, of order 3). This proves (ii) and completes the proof of Theorem 6.3.

It should perhaps be noted that the square-mapping (2) need not be a semi-automorphism of H. As an obvious example, consider the case that G is an infinite cyclic group.

At this point let us remark that (by SVII Lemma 5.1) the identities (6.1)—(6.5) are equivalent not only for Moufang loops but also for di-associative loops. This fact is important in connection with the following theorem:

THEOREM 6.4. *Let G be a di-associative loop without elements of order 2, in which (6.1) holds identically. Then there exists a loop G^* (uniquely defined to within an isomorphism leaving G elementwise fixed) such that:*

(i) *G is a subloop of G^*.*

(ii) *G^* is di-associative and has no elements of order 2.*

(ii) *The square-mapping (2) is a semi-automorphism of G^*.*

(iv) *If x is in G^*, there exists at least one power of 2, say p, such that x^p is in G.*

PROOF. First we note that, for x, y in G,

$$x^2 = y^2 \Leftrightarrow x = y. \tag{6.18}$$

Indeed, by (6.4), (6.3), $x^2 = y^2$ implies $(x\,y^{-1})^4 = (x, y^{-1})^{-6} = (x, y^2)^3 = 1$; and thence, since G has no elements of order 2, $x = y$.

In view of (6.18), square roots are unique in G if they exist. Consequently, by (i)—(iv), G^* should consist of the set of all elements $x^{1/p}$ where x ranges over G and p over the set

$$P = \{2^n;\ n = 0, 1, 2, \ldots\}. \tag{6.19}$$

We should expect to find, if indeed G^* satisfies (6.4), (6.3), that

$$\begin{aligned}(x^{1/p}\,y^{1/q})^{2pq} &= x^{2q}\,y^{2p}(x^{1/p}, y^{1/q})^{-pq(2pq-1)} \\ &= x^{2q}\,y^{2p}(x, y)^{1-2pq} = x^q\,y^{2p}\,x^q(x, y).\end{aligned}$$

This leads to the following formal definition:

G^* is obtained from the set-product $P \times G$ by imposing the equivalence relation

$$[p, x] = [q, y] \Leftrightarrow x^q = y^p. \tag{6.20}$$

the product rule

$$[p, x][q, y] = [2p\,q,\ x^q\, y^{2p}\, x^q (x, y)] \tag{6.21}$$

and the identification

$$[1, x] = x. \tag{6.22}$$

Straightforward computations, using (6.1)—(6.5) and (6.18) for G, show that G^*, as defined by (6.20)—(6.22), is a loop with the properties stated in Theorem 6.4.

Suppose, finally, that G is a *Moufang* loop satisfying (6.1) and without elements of order 2. Then G^* exists with properties (i)—(iv) of Theorem 6.4; but is G^* Moufang? If we assume that G^* is Moufang, we may conclude that G^* and G have the properties (i)—(iii) of Theorem 6.1. If we assume that G has the properties (i), (ii) of Lemma 6.1, we may show quite easily that G^* is Moufang. But in general it is by no means clear whether G^* is Moufang when G is.

References

[1] BRUCK, R. H.: A Survey of Binary Systems. Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, H. 20. Berlin-Göttingen-Heidelberg: Springer 1958. — [2] PAIGE, L. J.: A class of simple Moufang loops. Proc. Amer. Math. Soc. **7**, 471—482 (1956). MR **18**, 110. — [3] BRUCK, R. H.: Normal endomorphisms. Illinois J. Math. (To appear in March, 1960.)

Dept. of Math., University of Wisconsin, Madison 6, Wisconsin (USA)

(Eingegangen am 19. Juni 1959)

O'KEEFE, E. S.
Math. Zeitschr. 73, 79–94 (1960)

On the independence of primal algebras

By
EDWARD S. O'KEEFE

I. Introduction

The algebraic structure common to Boolean and Post algebras and to p-rings has recently been extended by A. L. FOSTER to a comprehensive structure theory for universal algebras. In the most general phase of this latter theory the concept *primal cluster* (of arbitrary species Sp) plays a central role. Each such cluster determines a unique sub-direct factorization for each algebra equationally embedded in the cluster, i.e., an algebra satisfying all identities common to some finite subset of the cluster. Various categories of primal clusters are known, largely clusters of species $[2,1.]$.

The principal objective of this paper is to establish new categories of primal clusters, thus broadening the domain of application of the general structure theory. It is shown, in particular, that the totality of pairwise non-isomorphic primal algebras of species $[s]$ constitute a primal cluster. Furthermore, the relationship between pairwise independence and independence for general algebras is clarified.

The following definitions are stated for easy reference.

Let $\mathfrak{A}=(A, o_1, o_2, \ldots)$ be a universal algebra.

1.1. The *species* $Sp=[n_1, n_2, \ldots]$ of $\mathfrak{A}$ is the sequence of ranks of the primitive operations o_i of $\mathfrak{A}$, where n_i is the rank of o_i.

1.2. An $\mathfrak{A}$-*function* is a composition by means of the primitive operations o_i of $\mathfrak{A}$, of elements of A and indeterminates over A.

1.3. An $\mathfrak{A}$-function is *strict* if it involves no constants, being a composition only of indeterminates over A.

1.4. $\mathfrak{A}$ is *functionally strictly complete* if every set-theoretic mapping of the class $A\times A\times\cdots\times A$ (k-th Cartesian power) into the set A can be represented as a strict $\mathfrak{A}$-function.

1.5. $\mathfrak{A}$ is said to be *primal* if A has more than one element and $\mathfrak{A}$ is functionally strictly complete.

1.6. An *expression* is a set of indeterminate symbols composed by operation-symbols. Each expression is associated with a species $[n_1, n_2, \ldots, n_s]$.

1.7. If Φ is an expression of the same species as algebra $\mathfrak{A}$, $\Phi(\mathfrak{A})$ or $\Phi(\mathrm{mod}\ \mathfrak{A})$ means Φ interpreted as a strict $\mathfrak{A}$-function. $\Phi_1=\Phi_2(\mathfrak{A})$ means that the strict $\mathfrak{A}$-functions represented by the expressions are equal for every value of the arguments of Φ_1 and Φ_2.

1.8. A finite class of algebras $\{\mathfrak{A}_1, \ldots, \mathfrak{A}_n\}$ all of the same species Sp is *strictly independent* if, corresponding to each set of n expressions $\{\Phi_i\}$ of species Sp, there is at least one expression X such that $\Phi_i = X(\mathfrak{A}_i)$. The special case of strict independence of pairs of algebras is discussed in the sequel, and where confusion might arise, the special case is called pairwise strict independence; the general case is called general strict independence.

1.9. $\widetilde{\mathfrak{A}}$ is a *primal cluster* if $\widetilde{\mathfrak{A}}$ is a class of primal algebras and every finite subclass of $\widetilde{\mathfrak{A}}$ is strictly independent.

2. Factorization: Φ-condition

An idea basic to many of the proofs in this work is the simple one of factorization of strict functions. Just as positive real functions may have non-unique factorization, for instance, $f(x) = \left(\sqrt{f(x)} \times \sqrt{f(x)}\right)$, so may strict functions in universal algebras permit various factorizations into strict functions. We proceed immediately to find a form of such factorization for primal algebras.

DEFINITION 2.1. Let $\mathfrak{A} = (A, \mathbf{o}_1, \ldots, \mathbf{o}_t)$ be a universal algebra. The algebra $\mathfrak{A}$ is said to satisfy the *range condition* if each primitive operation $\mathbf{o}_i$ of $\mathfrak{A}$ has A as its range. Equivalently, we may say, for every $\mathbf{o}_i$ of rank n_i, and every $\alpha \in A$, there is a set $\{\alpha_1, \ldots, \alpha_{n_i}\} \subseteq A$ such that

$$\mathbf{o}_i(\alpha_1, \ldots, \alpha_{n_i}) = \alpha. \tag{2.1}$$

LEMMA 2.2. *Let $\mathfrak{B} = (B, \mathbf{o}_1, \ldots, \mathbf{o}_t)$ be a primal algebra satisfying the range condition. Then for every strict $\mathfrak{B}$-function, $\Gamma(\xi)$, and for every $i \leq t$, there are strict $\mathfrak{B}$-functions $\psi_1(\xi), \ldots, \psi_s(\xi)$ such that*

$$\mathbf{o}_i\left(\psi_1(\xi), \ldots, \psi_s(\xi)\right) = \Gamma(\xi). \tag{2.2}$$

(Here, as throughout, $=$ denotes "identically equal", unless otherwise specified.)

PROOF. Let $\mathbf{o}_i$ be any operation of $\mathfrak{B}$ of rank s, and let $\Gamma(\xi)$ be any strict $\mathfrak{B}$-function. Order the elements of B, i.e., $B = \{\beta_1, \ldots, \beta_n\}$. For each β_j, select a set of elements $\xi_{1j}, \xi_{2j}, \ldots, \xi_{sj}$ of $\mathfrak{B}$ such that

$$\mathbf{o}_i(\xi_{1j}, \ldots, \xi_{sj}) = \Gamma(\beta_j) \qquad (j = 1, \ldots, n). \tag{2.3}$$

Now define the set of functions $\{g_k(\xi)\}$ by $g_k(\beta_j) = \beta_{kj}$ $(j = 1, \ldots, n)$. Thus $\{g_k(\xi)\}$ $(k = 1, \ldots, s)$ is a set of functions from B to B. Since $\mathfrak{B}$ is primal, there exist $\psi_k(\xi) = g_k(\xi)$ $(k = 1, \ldots, s)$, where $\psi_k(\xi)$ is a strict $\mathfrak{B}$-function for each k. But

$$\mathbf{o}_i\left(\psi_1(\xi), \ldots, \psi_s(\xi)\right) = \Gamma(\xi)\ (\mathfrak{B}) \tag{2.4}$$

since, for each β_j,

$$\mathbf{o}_i\left(\psi_1(\beta_j), \ldots, \psi_s(\beta_j)\right) = \mathbf{o}_i(\xi_{1j}, \ldots, \xi_{sj}) = \Gamma(\beta_j). \tag{2.5}$$

The next lemma applies directly to infinite algebras as well as finite algebras.

LEMMA 2.3. *Let* $\mathfrak{A} = (A, \mathfrak{o}_1, \ldots, \mathfrak{o}_t)$ *be a universal algebra. The following four conditions are equivalent:*

I. *Corresponding to each* $i \leqq t$, *there exist strict* $\mathfrak{A}$*-functions* $\psi_1(\xi), \ldots, \psi_s(\xi)$ *such that*

$$\mathfrak{o}_i\big(\psi_1(\xi), \ldots, \psi_s(\xi)\big) = \xi. \tag{2.6}$$

II. *Corresponding to each* $i \leqq t$ *and to each strict* $\mathfrak{A}$*-function,* $\Phi(\xi, \eta, \ldots, \zeta)$, *there exist strict* $\mathfrak{A}$*-functions* $\psi_1(\xi, \eta, \ldots, \zeta), \ldots, \psi_s(\xi, \eta, \ldots, \zeta)$ *such that*

$$\mathfrak{o}_i\big(\psi_1(\xi, \eta, \ldots, \zeta), \ldots, \psi_s(\xi, \eta, \ldots, \zeta)\big) = \Phi(\xi, \eta, \ldots, \zeta). \tag{2.7}$$

III. *For every strict* $\mathfrak{A}$*-function* $\mathsf{K}(\xi_1, \ldots, \xi_m)$, *provided that no variable* ξ_i *occurs twice in* K, *there exist strict* $\mathfrak{A}$*-functions* $\psi_1(\xi), \ldots, \psi_m(\xi)$, *such that*

$$\mathsf{K}\big(\psi_1(\xi), \ldots, \psi_m(\xi)\big) = \xi. \tag{2.8}$$

IV. *For every strict* $\mathfrak{A}$*-function* $\vartheta(\xi, \eta, \ldots, \zeta)$ *and every strict* $\mathfrak{A}$*-function* $\mathsf{K}(\xi_1, \ldots, \xi_m)$, *provided that no variable* ξ_i *occurs twice in* K, *there exist strict* $\mathfrak{A}$*-functions* $\psi_1(\xi, \eta, \ldots, \zeta), \ldots, \psi_m(\xi, \eta, \ldots, \zeta)$ *such that*

$$\mathsf{K}\big(\psi_1(\xi, \eta, \ldots, \zeta), \ldots, \psi_m(\xi, \eta, \ldots, \zeta)\big) = \mathfrak{o}_i(\xi, \eta, \ldots, \zeta). \tag{2.9}$$

PROOF. III and IV are equivalent, since III is a special case of IV, and conversely, IV is easily derived from III, by replacing ξ in (2.8) by $\vartheta(\xi, \eta, \ldots, \zeta)$ and redefining the $\psi_i(\xi, \eta, \ldots, \zeta)$ of (2.9) in an obvious way.

In the same way, I and II are equivalent. Moreover, I is a special case of III — take $\mathsf{K} = \vartheta_i(\xi_1, \xi_2, \ldots, \xi_s)$. Therefore, to complete the proof, it suffices to derive IV from I. The derivation is made easily by induction on the number of operation signs in K.

Let property I hold in an algebra $\mathfrak{A}$. First, if the K of IV involves no primitive operations, it is simply a single variable ξ_i, and, in this case, the desired conclusion (2.9) is trivially true — i.e., $\vartheta(\xi, \eta, \ldots, \zeta) = \vartheta(\xi, \eta, \ldots, \zeta)$. Assume then (induction hypothesis) that IV holds in $\mathfrak{A}$ for all K involving n or fewer occurrences of primitive operations. We shall show that IV then also holds if K involves $n+1$ occurrences of primitive operations.

Suppose $\mathsf{K}(\xi_1, \ldots, \xi_m)$ to be a strict $\mathfrak{A}$-function containing $n+1$ operation signs. For some $\mathfrak{o}_j$, $1 \leqq j \leqq t$, of rank s, and some strict $\mathfrak{A}$-functions $\mathsf{M}_1, \ldots, \mathsf{M}_s$:

$$\mathsf{K}(\xi_1, \ldots, \xi_m) \quad \text{is} \quad \mathfrak{o}_j(\mathsf{M}_1, \ldots, \mathsf{M}_s). \tag{2.10}$$

To denote the variables in M_i, we can write $\mathsf{M}_i = \mathsf{M}_i(\xi_{k_i}, \ldots, \xi_{z_i})$. Each of the strict $\mathfrak{A}$-functions $\mathsf{M}_1, \ldots, \mathsf{M}_s$ then has $n\,\big(=(n+1)-1\big)$ operation signs or less, and all variables $\xi_{k_i}, \ldots, \xi_{z_i}$ different; that is, no variable occurs twice. Therefore, $\mathsf{M}_1, \ldots, \mathsf{M}_s$ fit the induction hypothesis. There exist also strict $\mathfrak{A}$-functions $\psi_1(\xi, \eta, \ldots, \zeta)$, $\psi_2(\xi, \eta, \ldots, \zeta), \ldots, \psi_s(\xi, \eta, \ldots, \zeta)$ such that for the $\mathfrak{o}_j$ of (2.10),

$$\mathfrak{o}_j\big(\psi_1(\xi, \eta, \ldots, \zeta), \ldots, \psi_s(\xi, \eta, \ldots, \zeta)\big) = \vartheta(\xi, \eta, \ldots, \zeta). \tag{2.11}$$

(This existence follows since property I — and with it the equivalent property II — holds in $\mathfrak{A}$.)

Corresponding to each of the ψ_i, $(i = 1, \ldots, s)$, by the induction hypothesis, there exist a set of $\mathfrak{A}$-functions $\Phi_{k_i}, \ldots, \Phi_{e_i}$, which, when substituted for $\xi_{k_i}, \ldots, \xi_{e_i}$ in M_i, satisfy the identity

$$\psi_i(\xi, \eta, \ldots, \zeta) = \mathsf{M}_i\big(\Phi_{k_i}(\xi, \eta, \ldots, \zeta), \ldots, \Phi_{e_i}(\xi, \eta, \ldots, \zeta)\big). \tag{2.12}$$

Since no variable ξ_t occurs twice in K, Φ_t can be substituted for ξ_t $(t = 1, \ldots, m)$ throughout K without conflict.

The result is

$$\begin{cases} \mathsf{K}(\Phi_1, \ldots, \Phi_m) = \sigma_j\big(\mathsf{M}_1(\Phi_{k_1}, \ldots, \Phi_{e_1}), \ldots, \mathsf{M}_s(\Phi_{k_s}, \ldots, \Phi_{e_s})\big) \\ \qquad\qquad = \sigma_j(\psi_1, \ldots, \psi_s) = \vartheta. \end{cases} \tag{2.13}$$

Therefore, $\Phi_1, \ldots, \Phi_m$ is the required set and IV is proved.

Lemma 2.3 applies to many primal algebras and is the basis for much of the work which follows. For convenience of notation we make the following definition:

DEFINITION 2.4. Condition IV shall be referred to as the Φ-condition.

3. A Partial Result for Primal Algebras of Arbitrary Species

Let $\mathfrak{A} = (A, \sigma, \ldots)$ and $\mathfrak{B} = (B, \sigma, \ldots)$ be arbitrary primal algebras of the same species. Two elements $\alpha \in A$, $\beta \in B$ are called *co-constants* — in symbols $\alpha \sim \beta$ — if there exists an expression $\Phi(\xi)$ such that $\Phi(\xi) = \alpha(\mathfrak{A})$ and $\Phi(\xi) = \beta(\mathfrak{B})$. The occurrence of such pairs is common.

We use the following lemma from FOSTER [9].

LEMMA 3.0. *Let $\mathfrak{A}$ and $\mathfrak{B}$ be two primal, non-isomorphic algebras. Let β' and β'' be elements of $\mathfrak{B}$. Then there is always an element α of $\mathfrak{A}$ such that $\alpha \sim \beta'$ and $\alpha \sim \beta''$.*

We now prove a kind of generalization of this lemma.

THEOREM 3.1. *Let $\mathfrak{A} = (A, \sigma, \ldots)$ and $\mathfrak{B} = (B, \sigma, \ldots)$ be two non-isomorphic primal algebras of the same species, Sp. Then there exists a set of unary expressions $\{\Phi_i\} = \{\Phi_1, \ldots, \Phi_p\}$ of species Sp such that*

$$\Phi_1 = \Phi_2 = \cdots = \Phi_p(\mathfrak{A}) \tag{3.1}$$

and such that every unary $\mathfrak{B}$-function is equivalent modulo $\mathfrak{B}$ to one of the expressions $\Phi_1, \ldots, \Phi_p$.

PROOF. First consider the transformations of one argument of the class B into itself. Let these be numbered: $b_1(\xi), b_2(\xi), \ldots, b_p(\xi)$, where $p = n^n$, $n =$ order of B. Every strict $\mathfrak{B}$-function X which involves only one indeterminate ξ has a transformation $b_i(\xi)$ such that

$$X(\xi) = b_i(\xi). \tag{3.2}$$

Let β_1, β_2 be any distinct elements of B. Recalling that $\mathfrak{B}$ is primal, a strict $\mathfrak{B}$-function $\Phi(\xi, \xi_1, \ldots, \xi_{p+1})$ exists, satisfying the identities:

$$(3.3)\qquad \begin{cases} \Phi(\xi, \beta_1, \beta_2, \ldots, \beta_2) = b_1(\xi)\,(\mathfrak{B}) \\ \Phi(\xi, \beta_1, \beta_1, \beta_2, \ldots, \beta_2) = b_2(\xi)\,(\mathfrak{B}) \\ \qquad\vdots \\ \Phi(\xi, \beta_1, \beta_1, \ldots, \beta_1, \beta_2, \beta_2) = b_{p-1}(\xi)\,(\mathfrak{B}) \\ \Phi(\xi, \beta_1, \beta_1, \ldots, \beta_1, \beta_2) = b_p(\xi)\,(\mathfrak{B}). \end{cases}$$

That is, whenever $\xi_i = \beta_1$, $i \leqq j$ and $\xi_i = \beta_2$, $i > j$, then $\Phi(\xi, \beta_1, \ldots, \beta_1, \beta_2, \ldots, \beta_2) = b_j(\xi)\,(\mathfrak{B})$. By Lemma 3.0, there are expressions ψ_1, ψ_2 and an element α of $\mathfrak{A}$ such that

$$(3.4)\qquad \begin{cases} \psi_1(\xi) = \begin{cases} \alpha\,(\mathfrak{A}) \\ \beta_1(\mathfrak{B}) \end{cases} \\ \psi_2(\xi) = \begin{cases} \alpha\,(\mathfrak{A}) \\ \beta_2(\mathfrak{B}). \end{cases} \end{cases}$$

We use the Φ of (3.3) as a skeleton to construct the desired expressions Φ_j. Let

$$(3.5)\qquad \begin{cases} \Phi_1(\xi) = \Phi\big(\xi, \psi_1(\xi), \psi_2(\xi), \ldots, \psi_2(\xi)\big) \\ \Phi_2(\xi) = \Phi\big(\xi, \psi_1(\xi), \psi_1(\xi), \psi_2(\xi), \ldots, \psi_2(\xi)\big) \\ \qquad\vdots \\ \Phi_p(\xi) = \Phi\big(\xi, \psi_1(\xi), \ldots, \psi_1(\xi), \psi_2(\xi)\big). \end{cases}$$

Otherwise expressed, $\Phi_i(\xi) = \Phi\big(\xi, \psi_1(\xi), \ldots, \psi_2(\xi)\big)$ where $\psi_1(\xi)$ has been substituted for ξ_i, $1 \leqq i \leqq j$ and $\psi_2(\xi)$ has been substituted for ξ_i, $j < i < p+1$.

Using (3.3), (3.4), and (3.5) we have

$$(3.6)\qquad \Phi_j(\xi) = \Phi\big(\xi, \underbrace{\psi_1(\xi), \ldots, \psi_1}_{j\ \psi_1\text{'s}}(\xi), \psi_2(\xi), \ldots, \psi_2(\xi)\big) = b_j(\xi)\,(\mathfrak{B}).$$

The consequence is: If X is any strict $\mathfrak{B}$-function, involving no more than one indeterminate, we have from (3.2) and (3.6) for some j, $1 \leqq j \leqq m$

$$(3.7)\qquad \Phi_j = X(\mathfrak{B}).$$

We shall now prove (3.1).

In $\mathfrak{A}$, $\psi_1(\xi) = \psi_2(\xi)\,(\mathfrak{A})$. In fact, according to the selection of $\psi_1(\xi)$ and $\psi_2(\xi)$ in (3.4), $\psi_1(\xi) = \alpha\,(\mathfrak{A})$ and $\psi_2(\xi) = \alpha\,(\mathfrak{A})$. Thus by (3.5)

$$(3.8)\qquad \Phi_i(\xi) = \Phi(\xi, \alpha, \ldots, \alpha)\,(\mathfrak{A}) \qquad \text{for } i \leqq p+1.$$

Therefore

$$(3.9)\qquad \Phi_i(\xi) = \Phi_j(\xi)\,(\mathfrak{A}) \qquad (i, j \leqq p+1),$$

which completes the proof of Theorem 3.1.

4. Species [s]: Φ-condition, etc.

In primal algebras of species $[s]$, we observe a generalized factorization of elements, which leads to the Φ-condition (condition IV of Lemma 2.2) thus:

LEMMA 4.1. *Let $\mathfrak{A}=(A, o)$ be a primal algebra of species $[s]$. Then, for each $\alpha \in A$, there exists a sequence, $\{\alpha_1, \ldots, \alpha_s\} \subseteq A$, so that*

$$o(\alpha_1, \ldots, \alpha_s) = \alpha. \tag{4.1}$$

PROOF. Clearly, if, for some α, there is no such sequence, $(A-\{\alpha\}, o)$ is a proper subalgebra of $\mathfrak{A}$. This is impossible, since no primal algebra has a (proper) subalgebra. This establishes Lemma 4.1.

LEMMA 4.2. *The Φ-condition holds in every primal algebra of species $[s]$.*

PROOF. Lemma 4.1 shows that Lemma 2.2 applies to primal algebras of species $[s]$. Lemma 2.3 (holding for arbitrary universal algebras) states that the conclusion of Lemma 2.2 is equivalent to the Φ-condition. Therefore, the Φ-condition holds in primal algebras of species $[s]$, and the lemma is proved.

THEOREM 4.3. *Let $\mathfrak{A}=(A, o)$ $\mathfrak{B}=(B, o)$ be non-isomorphic primal algebras of species $[s]$. Corresponding to each $\alpha \in A$, and each strict $\mathfrak{B}$-function, $\psi(\xi)$, there exists an expression $X(\xi)$ such that*

$$X(\xi) = \begin{cases} \alpha\,(\mathfrak{A}) \\ \psi(\xi)\,(\mathfrak{B}). \end{cases} \tag{4.2}$$

PROOF. Let $\mathsf{K}(\xi)$ be any strict $\mathfrak{A}$-function such that

$$\mathsf{K}(\xi) = \alpha\,(\mathfrak{A}). \tag{4.3}$$

Let p be the number of occurrences of ξ in K. Replace each occurrence with a different variable from the set $\{\xi_1, \ldots, \xi_p\}$, thus separating the occurrences of ξ in K. Call the result $\mathsf{K}'(\xi_1, \ldots, \xi_p)$. Then

$$\mathsf{K}'(\xi, \xi, \ldots, \xi) = \mathsf{K}(\xi)\,(\mathfrak{A}). \tag{4.4}$$

By Lemma 4.2, the Φ-condition holds in the algebra $\mathfrak{B}$. So, there exist strict $\mathfrak{B}$-functions $\psi_1(\xi), \ldots, \psi_p(\xi)$ such that

$$\mathsf{K}'\big(\psi_1(\xi), \ldots, \psi_p(\xi)\big) = \psi(\xi)\,(\mathfrak{B}). \tag{4.5}$$

It is noted that Theorem 3.1 was established for a pair of primal algebras of arbitrary species. From Theorem 3.1, then, there exist strict expressions $\vartheta_1(\xi), \ldots, \vartheta_p(\xi)$ such that

$$\vartheta_i(\xi) = \vartheta_j(\xi)\,(\mathfrak{A}), \qquad 1 \leq i, j \leq p. \tag{4.6}$$

$$\vartheta_i(\xi) = \psi_i(\xi)\,(\mathfrak{B}), \qquad 1 \leq i \leq p. \tag{4.7}$$

Consider $\mathsf{K}'\big(\vartheta_1(\xi), \ldots, \vartheta_p(\xi)\big)$. By (4.6), then (4.4) and (4.3), we have

$$\begin{cases} \mathsf{K}'\big(\vartheta_1(\xi), \ldots, \vartheta_p(\xi)\big) = \mathsf{K}'\big(\vartheta_1(\xi), \ldots, \vartheta_1(\xi)\big)\,(\mathfrak{A}) \\ \qquad\qquad\qquad\qquad = \mathsf{K}\big(\vartheta_1(\xi)\big)\,(\mathfrak{A}) = \alpha\,(\mathfrak{A}). \end{cases} \tag{4.8}$$

But, by (4.7),

$$\mathsf{K}'\big(\vartheta_1(\xi),\ldots,\vartheta_p(\xi)\big) = \mathsf{K}'\big(\psi_1(\xi),\ldots,\psi_p(\xi)\big)(\mathfrak{B}) = \psi(\xi)(\mathfrak{B}), \tag{4.9}$$

where the last follows from (4.5). Therefore, $\mathsf{K}'\big(\vartheta_1(\xi),\ldots,\vartheta_p(\xi)\big)$ has the properties predicted in formula (4.2). This concludes the proof of Theorem 4.3.

DEFINITION. Let T denote the cyclic permutation of arguments of a primitive operation, o, and T^n its n-th iteration,

$$o^{T^n}(\xi_1,\ldots,\xi_s)\,(=o^{(n)}) = o(\xi_{n+1},\ldots,\xi_s,\xi_1,\ldots,\xi_n), \tag{4.10}$$

in particular,

$$o^{T^s}(=o^{(0)}) = o. \tag{4.11}$$

LEMMA 4.4. *(Separation Lemma for Species [s].) Let $\mathfrak{A}=(A,o)$ be a primal algebra of species [s]. For each non-constant $\mathfrak{A}$-function, $f(\xi)$, there is a set, $\{\gamma_1,\ldots,\gamma_{s-1}\}\in A$, and a number n, $0\leqq n\leqq s-1$, such that $o^{(n)}\big(f(\xi),\gamma_1,\ldots,\gamma_{s-1}\big)$ is not a constant.*

PROOF. Let $f(\eta)$ be some non-constant $\mathfrak{A}$-function i.e., for some α_1,α_2, $\beta_1,\beta_2\in A$,

$$f(\alpha_1)=\alpha_2\neq f(\beta_1)=\beta_2. \tag{4.12}$$

Suppose the lemma false, then, for every sequence, $\gamma_1,\ldots,\gamma_{s-1}$ and every n,

$$o^{(n)}(\alpha_2,\gamma_1,\ldots,\gamma_{s-1}) = o^{(n)}(\beta_2,\gamma_1,\ldots,\gamma_{s-1}). \tag{4.13}$$

Since this holds for arbitrary $\gamma_1,\ldots,\gamma_{s-1}\in\mathfrak{A}$ and for all $n=1,\ldots,s$, (4.13) now asserts that for given j, $1\leqq j\leqq s$,

$$o(\xi_1,\ldots,\xi_{j-1},\alpha_2,\xi_{j+1},\ldots,\xi_s) = o(\xi_1,\ldots,\xi_{j-1},\beta_2,\xi_{j+1},\ldots,\xi_s). \tag{4.14}$$

If, on the one hand, A consists of only the two elements α_2,β_2, then (4.14) implies that o is a constant operation. On the other hand, if A has more than two elements, the mapping sending α_2 into β_2, β_2 into β_2 and every other element into itself, is a non-trivial homomorphism, which is impossible for a primal algebra. These contradictions prove Lemma 4.4.

THEOREM 4.5. *Let $\mathfrak{A}=(A,o)$ and $\mathfrak{B}=(B,o)$ be two non-isomorphic primal algebras of species [s]. There is an expression $\Omega(\xi,\eta)$, which is equivalent to ξ modulo $\mathfrak{B}$, and to some non-constant function of η modulo $\mathfrak{A}$.*

PROOF. First choose integers a_i and elements $\alpha_{i,j}$ of A such that the $\mathfrak{A}$-function $\pi_i(\eta)$ $(i=1,2,\ldots)$ defined by

$$\pi_1(\eta) = o^{a_1}(\eta,\alpha_{1,2},\ldots,\alpha_{1,s}) \tag{4.15}$$

and

$$\pi_{i+1}(\eta) = o^{a_{i+1}}\big(\pi_i(\eta),\alpha_{i+1,2},\ldots,\alpha_{i+1,s}\big) \tag{4.16}$$

are all non-constant.

Secondly, let β be any element of B, and let $\Sigma(\xi,\zeta)$ be an expression of species $[s]$ such that

$$\Sigma(\beta,\zeta)=\zeta \qquad (\mathrm{mod}\ \mathfrak{B}) \tag{4.17}$$

and

$$\Sigma(\xi,\beta)=\xi \qquad (\mathrm{mod}\ \mathfrak{B}). \tag{4.18}$$

If d is an integer larger than the number of occurrences of the σ operation in $\Sigma(\xi,\zeta)$, we can find an integer c, $0<c<d$, and expressions $\Sigma_i=\Sigma_i(\xi,\zeta)$, $\vartheta_{i,j}=\vartheta_{i,j}(\xi,\zeta)$ such that

$$\Sigma=\Sigma_d, \tag{4.19}$$

$$\Sigma_{i-1}=\sigma^{a_{i+1}}(\Sigma_i,\vartheta_{i+1,2},\ldots,\vartheta_{i+1,s}) \qquad (i=c,\ c+1,\ldots,d+1), \tag{4.20}$$

$$\Sigma_c=\xi \quad \text{or} \quad \Sigma_c=\zeta. \tag{4.21}$$

After a possible redefinition of Σ, Σ_i and $\vartheta_{i,j}$, so that the first and second variables are interchanged, we can assume that

$$\Sigma_c=\zeta. \tag{4.22}$$

According to Theorem 4.3, there exist $\Phi(\eta)$, $X_{i,j}(\xi)$ such that

$$\Phi(\eta)=\begin{cases}\pi_c(\eta) & (\mathfrak{A})\\ \beta & (\mathfrak{B}),\end{cases} \tag{4.23}$$

$$X_{i,j}(\xi)=\begin{cases}\alpha_{i,j} & (\mathfrak{A})\\ \vartheta_{i,j}(\xi,\beta) & (\mathfrak{B}).\end{cases} \tag{4.24}$$

Define $\Omega_i=\Omega_i(\xi,\eta)$, $(i=c,\ldots,d)$ by

$$\Omega_c=\Phi(\eta), \tag{4.25}$$

$$\Omega_{i-1}=\sigma^{(a_{i+1})}(\Omega_i,X_{i+1,2},\ldots,X_{i+1,s}). \tag{4.26}$$

Since

$$\Omega_i=\begin{cases}\pi_i(\eta) & (\mathfrak{A})\\ \Sigma_i(\xi,\beta) & (\mathfrak{B}),\end{cases} \tag{4.27}$$

then

$$\Omega_d(\xi,\zeta)=\begin{cases}\pi_d(\eta) & (\mathfrak{A})\\ \xi & (\mathfrak{B}).\end{cases} \tag{4.28}$$

This completes the proof of Theorem 4.5.

5. Basic Independence Theorem for Species [s]

Much of the preceding theory serves as a foundation for the Basic Independence Theorem for Species $[s]$ (Theorem 5.2), which we now consider.

With reference to Theorem 4.5, the non-constancy of $\Pi(\eta)$ asserts that there are at least two elements $\gamma_0,\gamma_1\in A$ in the range of $\Pi(\eta)$. Now, since $\mathfrak{A}$

is primal, if $\psi_0(\eta)$ is any expression whose range, modulo $\mathfrak{A}$, is restricted to those two elements, there exists an expression $\Gamma_2(\eta)$ such that

$$\Pi\big(\Gamma_2(\eta)\big) = \psi_0(\eta)\,(\mathfrak{A})\,. \tag{5.1}$$

Furthermore, if $\psi_1(\xi)$ is any expression, we have, for the expression Ω discussed in Theorem 4.5,

$$\Omega\big(\psi_1(\xi), \Gamma_2(\eta)\big) = \begin{cases} \psi_0(\eta)\,(\mathfrak{A}) \\ \psi_1(\xi)\,(\mathfrak{B})\,. \end{cases} \tag{5.2}$$

We state the above conclusions as

LEMMA 5.1. *Let $\mathfrak{A} = (A, \mathfrak{o})$ and $\mathfrak{B} = (B, \mathfrak{o})$ be two non-isomorphic primal algebras of species $[s]$. There exist two elements $\gamma_0, \gamma_1 (\gamma_0 \neq \gamma_1)$ of A such that if $\psi_0(\eta)$ is an $\mathfrak{A}$-function whose range is restricted to $\{\gamma_0, \gamma_1\}$ and $\psi_1(\xi)$ is an arbitrary $\mathfrak{B}$-function, then we can find an expression $\Delta(\xi, \eta)$ satisfying*

$$\Delta(\xi, \eta) = \begin{cases} \psi_0(\eta)\,(\mathfrak{A}) \\ \psi_1(\xi)\,(\mathfrak{B})\,. \end{cases} \tag{5.3}$$

It is now possible to prove:

THEOREM 5.2. *(Basic Independence Theorem for Species $[s]$.) If $\mathfrak{A} = (A, \mathfrak{o})$ and $\mathfrak{B} = (B, \mathfrak{o})$ are two non-isomorphic primal algebras of species $[s]$, then they are strictly independent.*

PROOF. Let $A = \{\alpha_1, \ldots, \alpha_n\}$, and let γ_0, γ_1 be distinct elements of A satisfying Corollary 5.1. Let $\Xi(\xi_1, \ldots, \xi_{n+1})$ be an expression with the following properties:

$$\begin{cases} \Xi(\gamma_0, \gamma_1, \ldots, \gamma_1) = \alpha_1\,(\mathfrak{A}) \\ \Xi(\gamma_0, \gamma_0, \gamma_1, \ldots, \gamma_1) = \alpha_2\,(\mathfrak{A}) \\ \qquad\qquad \vdots \\ \Xi(\gamma_0, \gamma_0, \ldots, \gamma_0, \gamma_1, \gamma_1) = \alpha_{n-1}\,(\mathfrak{A}) \\ \Xi(\gamma_0, \gamma_0, \ldots, \gamma_0, \gamma_1) = \alpha_n\,(\mathfrak{A})\,. \end{cases} \tag{5.4}$$

That is, if γ_0 is substituted for ξ_j, whenever $j \leqq i \leqq n$, and γ_1 for the remaining ξ_j's, we are to have

$$\Xi(\gamma_0, \ldots, \gamma_1) = \alpha_i\,(\mathfrak{A})\,. \tag{5.5}$$

The values of Ξ for other values of the arguments are immaterial, as will be seen.

For each i, replace the various occurrences of ξ_i in Ξ by the variables $\xi_{i,0}, \xi_{i,1}, \ldots$, thus separating the occurrences of each variable. We get a new expression

$$\Xi'(\xi_{1,0}, \xi_{1,1}, \ldots, \xi_{2,0}, \ldots, \xi_{n+1,m}) \tag{5.6}$$

in which no variable occurs twice. By Lemma 4.2, the Φ-condition holds with respect to algebra $\mathfrak{B}$. Therefore, there are strict $\mathfrak{B}$-functions, $\psi_{j,k}(\xi)$, $(j = 1, 2, \ldots, n+1)$, such that

$$\Xi'\big(\psi_{1,0}(\xi), \ldots, \psi_{2,0}(\xi), \ldots, \psi_{n+1,m}(\xi)\big) = \xi\,(\mathfrak{B})\,. \tag{5.7}$$

Moreover, by Corollary 5.1, there exist expressions $\Delta_{j,k}(\xi,\eta)$, for which not only

$$\Delta_{j,k}(\xi,\eta) = \psi_{j,k}(\xi)\,(\mathfrak{B}) \tag{5.8}$$

but also

$$\Delta_{j,k}(\xi,\alpha_i) = \begin{cases} \gamma_0(\mathfrak{A}) & \text{for } j \leqq i \\ \gamma_1(\mathfrak{A}) & \text{for } j > i. \end{cases} \tag{5.9}$$

Then, replacing each $\xi_{j,k}$ by $\Delta_{j,k}(\xi,\eta)$ in Ξ', for given α_i

$$\begin{cases} \Xi'\big(\Delta_{1,0}(\xi,\alpha_i),\ldots,\Delta_{2,0}(\xi,\alpha_i),\ldots,\Delta_{n+1,m}(\xi,\alpha_i)\big) \\ \qquad = \Xi'(\gamma_0,\ldots,\gamma_0,\gamma_1,\ldots,\gamma_1)\,(\mathfrak{A}) = \alpha_i(\mathfrak{A}), \end{cases} \tag{5.10}$$

where the last step results from (5.4) and (5.6) on replacing Ξ' by the corresponding unseparated Ξ.

By (5.10) we have

$$\Xi'\big(\Delta_{1,0}(\xi,\eta),\ldots,\Delta_{2,0}(\xi,\eta),\ldots,\Delta_{n+1,m}(\xi,\eta)\big) = \eta(\mathfrak{A}). \tag{5.11}$$

By (5.7) and (5.8),

$$\begin{cases} \Xi'\big(\Delta_{1,0}(\xi,\eta),\ldots,\Delta_{2,0}(\xi,\eta),\ldots,\Delta_{n+1,m}(\xi,\eta)\big) \\ \qquad = \Xi\big(\psi_{1,0}(\xi),\ldots,\psi_{2,0}(\xi),\ldots,\psi_{n+1,m}(\xi)\big)\,(\mathfrak{B}) = \xi(\mathfrak{B}). \end{cases} \tag{5.12}$$

The properties (5.11), (5.12) of the expression Ξ' complete the proof of Theorem 5.2.

6. General Independence

The basic result on the independence of a pair of non-isomorphic primal algebras of species $[s]$ is now complete. In the present section, we shall extend this result to classes of such primal algebras, and shall show in particular, that for primal algebras (of species $[s]$), pairwise independence implies general independence. Before establishing this result, we shall, however, engage in a more general discussion of independence, applicable to arbitrary algebras, satisfying the Φ-condition. The derivation of general strict independence from pairwise strict independence is naturally made by induction. The general step in the induction is facilitated by the following lemma.

LEMMA 6.1. *Let $\{\mathfrak{A}_1,\ldots,\mathfrak{A}_{n-1}\}$ be a finite class of algebras of the same species, Sp, in which every proper sub-class is independent. There exist (fixed) expressions, $\alpha_1(\xi),\ \ldots,\ \alpha_n(\xi)$ with the property:*

Corresponding to each $\vartheta(\eta)$ and each $j \leqq n$, there exists an expression $\psi(\xi,\eta)$ of species Sp, such that

$$\psi(\xi,\eta) = \begin{cases} \alpha_j(\xi)\,(\mathfrak{A}_j) \\ \xi\,(\mathfrak{A}_i) \qquad i = 1,\ldots,n;\ i \neq j. \\ \vartheta\,(\eta)\,(\mathfrak{A}_{n+1}) \end{cases} \tag{6.1}$$

PROOF. Select a set of expressions $\mathsf{K}_j(\xi, \eta)$ of species Sp such that

$$\mathsf{K}_j(\xi, \eta) = \begin{cases} \xi(\mathfrak{A}_i) & i = 1, \ldots, n;\ i \neq j \\ \eta(\mathfrak{A}_{n+1}). \end{cases} \tag{6.2}$$

Then for each j, define

$$\alpha_j(\xi) = \mathsf{K}_j(\xi, \xi)(\mathfrak{A}_j). \tag{6.3}$$

Let $\vartheta(\eta)$ be any $\mathfrak{A}_{n+1}$-function. Let $\Pi_j(\xi, \eta)$ be any expression of species Sp such that

$$\Pi_j(\xi, \eta) = \begin{cases} \xi(\mathfrak{A}_j) \\ \vartheta(\eta)(\mathfrak{A}_{n+1}). \end{cases} \tag{6.4}$$

Putting these expressions together, we have by (6.3), (6.4)

$$\mathsf{K}_j\big(\xi, \Pi_j(\xi, \eta)\big) = \begin{cases} \alpha_j(\xi)(\mathfrak{A}_j) \\ \xi(\mathfrak{A}_i) \\ \vartheta(\eta)(\mathfrak{A}_{n+1}). \end{cases} \tag{6.5}$$

Notice that $\mathsf{K}_j(\xi, \eta)$ need not vary for different ϑ's. Therefore, $\alpha_j(\xi)$ is dependent only on j — and not on the choice of ϑ. This concludes Lemma 6.1.

THEOREM 6.2. *Let $\{\mathfrak{A}_1, \ldots, \mathfrak{A}_n\}$ be a set of universal algebras of species Sp, in which every pair of algebras is strictly independent. If the Φ-condition holds in each algebra, the class is strictly independent.*

The proof will be by induction. The general step may be phrased as follows:

Let $\{\mathfrak{A}_1, \ldots, \mathfrak{A}_{n+1}\}$ $(n \geqq 2)$ be a class of universal algebras of species Sp, in which every proper subclass is a strictly independent class, and the Φ-condition holds in each algebra. The class is strictly independent.

PROOF. Let K be an expression of species Sp, such that

$$\mathsf{K}(\xi_1, \ldots, \xi_n) = \xi_i(\mathfrak{A}_i) \qquad (i = 1, \ldots, n). \tag{6.6}$$

Separate the occurrences of the variables in K, replacing ξ_1 by $\xi_{1,1}, \ldots, \xi_{l,1}$; ξ_2 by $\xi_{1,2}, \ldots, \xi_{m,2}$, and so on, making

$$\mathsf{K}'(\xi_{1,1}, \ldots, \xi_{l,1}, \xi_{1,2}, \ldots, \xi_{m,2}, \ldots, \xi_{1,n}, \ldots, \xi_{p,n}). \tag{6.7}$$

Since the Φ-condition holds in $\mathfrak{A}_{n+1}$, there exists a set $\{\vartheta_{j,k}(\xi_{n+1})\}$ of expressions for which

$$\mathsf{K}'(\vartheta_{1,1}, \ldots, \vartheta_{l,1}\vartheta_{1,2}, \ldots, \vartheta_{m,2}, \vartheta, \ldots, \vartheta_{1,n}, \ldots, \vartheta_{p,n}) = \xi_{n+1}(\mathfrak{A}_{n+1}). \tag{6.8}$$

For each pair, j, k, there exists, by the preceding lemma, an expression $\psi_{j,k}(\xi_k, \xi_{n+1})$ such that, for $k = 1$,

$$\psi_{j,1} = \begin{cases} \alpha_2(\xi_1)(\mathfrak{A}_2) \\ \xi_1(\mathfrak{A}_i) & i = 1, \ldots, n;\ \ i \neq 2 \\ \vartheta_{j,k}(\xi_{n+1})(\mathfrak{A}_{n+1}) \end{cases} \tag{6.9}$$

and for $k \neq 1$,

$$\psi_{j,k}(\xi_k, \xi_{n+1}) = \begin{cases} \alpha_1(\xi_k)\,(\mathfrak{A}_1) \\ \xi_k(\mathfrak{A}_i) \qquad\qquad (i = 2, 3, \ldots, n). \\ \vartheta_{j,k}(\xi_{n+1})\,(\mathfrak{A}_{n+1}) \end{cases} \tag{6.10}$$

In K', substitute $\psi_{j,k}$ for $\xi_{j,k}$, calling the result $\mathsf{K}''(\xi_1, \ldots, \xi_{n+1})$

$$\begin{cases} \mathsf{K}''(\xi_1, \ldots, \xi_{n+1}) \\ = \mathsf{K}'\big(\psi_{1,1}(\xi_1, \xi_{n+1}), \ldots, \psi_{l,1}(\xi_1, \xi_{n+1}), \ldots, \psi_{1,n}(\xi_n, \xi_{n+1}), \ldots \\ \qquad\qquad \ldots, \psi_{p,n}(\xi_n, \xi_{n+1})\big). \end{cases} \tag{6.11}$$

Then by (6.9), (6.10),

$$\mathsf{K}'' = \mathsf{K}'\big(\xi_1, \ldots, \xi_1, \alpha_1(\xi_2), \ldots, \alpha_1(\xi_n)\big) = \xi_1(\mathfrak{A}_1). \tag{6.12}$$

Also by (6.9) and (6.10)

$$\mathsf{K}'' = \mathsf{K}'\big(\alpha_2(\xi_1), \ldots, \alpha_2(\xi_1), \xi_2, \ldots, \xi_2, \xi_3, \ldots, \xi_3, \ldots, \xi_n, \ldots, \xi_n\big) = \xi_2(\mathfrak{A}_2). \tag{6.13}$$

And, by the same reductions

$$\mathsf{K}'' = \mathsf{K}(\xi_1, \ldots, \xi_n) = \xi_i(\mathfrak{A}_i), \qquad (i = 3, \ldots, n). \tag{6.14}$$

By (6.9), (6.10), and then (6.8),

$$\mathsf{K}'' = \mathsf{K}'(\vartheta_{1,1}, \ldots, \vartheta_{l,1}, \ldots, \vartheta_{1,n}, \ldots, \vartheta_{p,n}) = \xi_{n+1}(\mathfrak{A}_{n+1}). \tag{6.15}$$

By (6.12) and (6.15)

$$\mathsf{K}'' = \xi_i(\mathfrak{A}_i) \qquad (i = 1, 2, \ldots, n+1), \tag{6.16}$$

concluding the proof of Theorem 6.2.

We apply the foregoing theorem immediately to primal algebras which fulfill the range condition (2.1).

Let $\mathfrak{A} = (A, \mathbf{o}_1, \ldots, \mathbf{o}_l)$ be a primal algebra. If each primitive operation $\mathbf{o}_i$ has A for its range, that is, $\mathbf{o}_i$ fulfills the range condition, then by Lemmas 2.2 and 2.3, the Φ-condition holds in $\mathfrak{A}$. This fact together with 6.3 yields as a corollary:

THEOREM 6.3. *Let $\{\mathfrak{A}_1, \ldots, \mathfrak{A}_n\}$ be a finite set of primal algebras of the same species Sp. If each algebra satisfies the range condition, and if each pair $\{\mathfrak{A}_i, \mathfrak{A}_j\}$, $i \neq j$, of algebras is strictly independent, then $\{\mathfrak{A}_1, \ldots, \mathfrak{A}_n\}$ is a strictly independent class.*

A second corollary materially extends the scope of application of the basic structure results for primal clusters.

THEOREM 6.4. *(Fundamental Theorem on Primal Clusters of Species [s].) Let $\{\mathfrak{A}_1, \ldots, \mathfrak{A}_n\}$, $\mathfrak{A}_i = (A_i, \mathbf{o})$ be a set of primal algebras of species [s]. If no two algebras are isomorphic, the class is a primal cluster.*

PROOF. By Lemma 4.2 and Theorem 5.2, Theorem 6.3 applies to each finite set of primal algebras of species [s]. This proves Theorem 6.4.

7. Pairwise vs. General Independence, etc.

In several investigations it has turned out that pairwise strict independence among the algebras of a finite set already implies their strict independence. This implication holds in coframal primal algebras, see FOSTER [9]. The Chinese Remainder Theorem is another example, as is demonstrated in [9]. Three further instances of this implication have, moreover, arisen in the present paper: primal algebras of one operation, primal algebras satisfying the range condition, and all algebras satisfying the Φ-condition[1]).

Under these conditions it seems natural to expect that pairwise strict independence (for a finite set of algebras) always implies strict independence. However, this is false, as will be shown by the following counter example.

THEOREM 7.1. *There exists a finite class of algebras which* i) *are pairwise independent, and which* ii) *satisfy the range condition, yet* iii) *are not independent.*

PROOF. Let three algebras be defined as follows:

(7.1) $$\mathfrak{A}_1 = \left(\{\alpha_1, \beta_1, \gamma_1\},\ \mathfrak{o}_1, \mathfrak{o}_2, \mathfrak{o}_3\right)$$

$$\mathfrak{o}_1(\xi, \eta) = \xi(\mathfrak{A}_1)$$

$$\mathfrak{o}_2(\xi, \eta) = \eta(\mathfrak{A}_1)$$

$\mathfrak{o}_3$ has the table:

$\mathfrak{o}_3$	α_1	β_1	γ_1
α_1	β_1	β_1	α_1
β_1	β_1	β_1	β_1
γ_1	γ_1	β_1	β_1

(7.2) $$\mathfrak{A}_2 = \left(\{\alpha_2, \beta_2, \gamma_2\},\ \mathfrak{o}_1, \mathfrak{o}_2, \mathfrak{o}_3\right).$$

$\mathfrak{o}_1$ has the table:

$\mathfrak{o}_1$	α_2	β_2	γ_2
α_2	β_2	β_2	α_2
β_2	β_2	β_2	β_2
γ_2	γ_2	β_2	β_2

$$\mathfrak{o}_2(\xi, \eta) = \xi(\mathfrak{A}_2)$$

$$\mathfrak{o}_3(\xi, \eta) = \eta(\mathfrak{A}_2)$$

(7.3) $$\mathfrak{A}_3 = \left(\{\alpha_3, \beta_3, \gamma_3\},\ \mathfrak{o}_1, \mathfrak{o}_2, \mathfrak{o}_3\right)$$

$$\mathfrak{o}_1(\xi, \eta) = \eta(\mathfrak{A}_3)$$

---

[1]) In the latter class fall finite groups which can be treated by an easy application of the Φ-condition, and are independent if and only if the orders are relatively prime. A similar result (without Φ-condition) is known to hold for certain other classes of universal algebras.

o_2 has the table:

o_2	α_3	β_3	γ_3
α_3	β_3	β_3	α_3
β_3	β_3	β_3	β_3
γ_3	γ_3	β_3	β_3

$$o_3(\xi,\eta)=\xi(\mathfrak{A}_3).$$

PROOF of i):

$$o_1(\xi,\eta)=\begin{cases}\xi(\mathfrak{A}_1)\\ \eta(\mathfrak{A}_3)\end{cases} \tag{7.4}$$

so $\mathfrak{A}_1$, $\mathfrak{A}_3$ are strictly independent. Similarly,

$$o_2(\xi,\eta)=\begin{cases}\eta(\mathfrak{A}_1)\\ \xi(\mathfrak{A}_2),\end{cases} \tag{7.5}$$

so $\mathfrak{A}_1$, $\mathfrak{A}_2$ are strictly independent.

$$o_3(\xi,\eta)=\begin{cases}\eta(\mathfrak{A}_2)\\ \xi(\mathfrak{A}_3),\end{cases} \tag{7.6}$$

concluding the proof of i).

PROOF of ii). ii) is clearly true since every element of each algebra appears in the range of identity functions and in the table of the tabulated functions.

PROOF of iii). The only $\mathfrak{A}_1$-functions in the single variable ξ, which can be represented as strict $\mathfrak{A}_1$-functions are ξ and β_1. That is,

$$\begin{cases} o_1(\xi,\xi)=o_1(\xi,\beta_1)=\xi(\mathfrak{A}_1)\\ o_1(\beta_1,\xi)=o_1(\beta_1,\beta_1)=\beta_1(\mathfrak{A}_1)\\ o_2(\xi,\xi)=o_2(\beta_1,\xi)=\xi(\mathfrak{A}_1)\\ o_2(\xi,\beta_1)=o_2(\beta_1,\beta_1)=\beta_1(\mathfrak{A}_1)\\ o_3(\xi,\xi)=o_3(\xi,\beta_1)=o_3(\beta_1,\xi)=o_3(\beta_1,\beta_1)=\beta_1(\mathfrak{A}_1). \end{cases} \tag{7.7}$$

Observe, in addition, that in $\mathfrak{A}_1$, for each pair $f(\xi)$, $g(\xi)$ of strict $\mathfrak{A}_1$-functions,

$$o_3\big(f(\xi),g(\xi)\big)=\beta_1(\mathfrak{A}_1). \tag{7.8}$$

Similarly in $\mathfrak{A}_2$ and $\mathfrak{A}_3$, ξ and β_i are the only $\mathfrak{A}_i$-functions representable as strict $\mathfrak{A}_i$-functions $(i=2,3)$. Moreover, for any expressions $f(\xi)$, $g(\xi)$.

$$o_1\big(f(\xi),g(\xi)\big)=\beta_2(\mathfrak{A}_2), \tag{7.9}$$

$$o_2\big(f(\xi),g(\xi)\big)=\beta_3(\mathfrak{A}_3). \tag{7.10}$$

Suppose the algebra strictly independent. There is then an expression of species $[2,2,2]$, $\mathsf{K}(\xi_1,\xi_2,\xi_3)$ such that

$$\mathsf{K}(\xi_1,\xi_2,\xi_3)=\xi_i(\mathfrak{A}_i), \qquad (i=1,2,3). \tag{7.11}$$

K must obviously by composite.

$$\mathsf{K}(\xi,\xi,\xi)=\xi(\mathfrak{A}_i), \qquad (i=1,2,3). \tag{7.12}$$

But, of course, $\mathsf{K}(\xi, \xi, \xi)$ is also composite. This means it is of the form of the left-hand side of (7.8), (7.9), or (7.10). But then

$$(7.13)\qquad \begin{cases} \mathsf{K}(\xi,\xi,\xi) = \beta_1(\mathfrak{A}) \\ \text{or} \quad \mathsf{K}(\xi,\xi,\xi) = \beta_2(\mathfrak{A}_2) \\ \text{or} \quad \mathsf{K}(\xi,\xi,\xi) = \beta_3(\mathfrak{A}_3) \end{cases}$$

which contradicts (7.12). This concludes the proof of Theorem 7.1.

The Φ-condition is not a necessary condition for independence since coframal primal algebras are independent without necessarily satisfying it, see [9]. However, a limited form of a related condition (condition I of Lemma 2.3) is necessary for independence, according to

THEOREM 7.2. *Let* $\{\mathfrak{A}_1, \ldots, \mathfrak{A}_n\}$, $\mathfrak{A}_i = (A_i, \mathbf{o}_1, \ldots, \mathbf{o}_t)$ *be a strictly independent set of algebras of species* $Sp = [n_1, \ldots, n_t]$. *For at least one* i *there exist expressions* $\Delta_1(\xi), \ldots, \Delta_{n_i}(\xi)$, *such that*

$$(7.14)\qquad \mathbf{o}_i\big(\Delta_1(\xi), \ldots, \Delta_{n_i}(\xi)\big) = \xi(\mathfrak{A}_j) \qquad (j = 1, \ldots, n).$$

PROOF. There exists some expression K of species Sp such that

$$(7.15)\qquad \mathsf{K}(\xi_1, \ldots, \xi_n) = \xi_j(\mathfrak{A}_j) \qquad (j = 1, \ldots, n).$$

In particular,

$$(7.16)\qquad \mathsf{K}(\xi, \ldots, \xi) = \xi(\mathfrak{A}_j) \qquad (j = 1, \ldots, n).$$

For some $\mathbf{o}_i$, and some expression $\Delta_1, \ldots, \Delta_{n_i}$,

$$(7.17)\qquad \mathsf{K}(\xi, \ldots, \xi) = \mathbf{o}_i\big(\Delta_1(\xi), \ldots, \Delta_{n_i}(\xi)\big).$$

By (7.16) and (7.17) we have

$$(7.18)\qquad \mathbf{o}_i\big(\Delta_1(\xi), \ldots, \Delta_{n_i}(\xi)\big) = \xi(A_j), \qquad (j = 1, \ldots, n),$$

concluding the proof of Theorem 7.2.

REMARKS. If $(P_n, x, \hat{})$ is the Post algebra of order n, known to be primal, then letting $\xi + \eta = \xi\hat{} \times \eta\hat{}$, $(P_n, +)$ is a primal algebra, since the old operations can be defined in terms of the new. Thus there is at least one primal algebra of every order greater than 1, and of every species having a binary (or indeed n-ary, $n > 1$), operation.

If the range condition remains unsatisfied, it is easy to find a set of primal algebras which are pairwise – but not generally – independent. Thus, for example, let

$$\mathfrak{A}_1 = (A_1, \mathbf{o}_1, \mathbf{o}_2, \mathbf{o}_3), \qquad \mathfrak{A}_2 = (A_2, \mathbf{o}_1, \mathbf{o}_2, \mathbf{o}_3), \qquad \mathfrak{A}_3 = (A_3, \mathbf{o}_1, \mathbf{o}_2, \mathbf{o}_3)$$

be algebras of species [2, 2, 2] with the following properties:

P. 1. $(A_1, \mathbf{o}_2)$ and $(A_3, \mathbf{o}_2)$ are non-isomorphic and primal, as is the pair $(A_1, \mathbf{o}_3)$ and $(A_2, \mathbf{o}_3)$, and the pair $(A_2, \mathbf{o}_1)$ and $(A_3, \mathbf{o}_1)$.

*P.*2. Modulo $\mathfrak{A}_i$, o_i lacks some element in its range $(i = 1, 2, 3)$.

By P. 1, $\mathfrak{A}_1$ and $\mathfrak{A}_3$ are independent, since the necessary strict functions can be constructed without even using o_1 or o_3. Similarly the other pairs $\mathfrak{A}_1$ and $\mathfrak{A}_2$, $\mathfrak{A}_2$ and $\mathfrak{A}_3$, are independent.

By P. 2, one can see that whatever expressions $\Delta_1(\xi)$, $\Delta_2(\xi)$ may be,

$$o_i\big(\Delta_1(\xi), \Delta_2(\xi)\big) \neq \xi(A_i) \qquad (i = 1, 2, 3). \tag{7.18}$$

Thus we have pairwise independence, without the necessary condition for independence of Theorem 7.2. Therefore the algebras are not independent.

Bibliography

[1] STONE, M. H.: The Theory of Representations of Boolean Algebras. Trans. Amer. Math. Soc. **40**, 37–111 (1936). – [2] McCOY, N. H., and DEANE MONTGOMERY: A Representation of Generalized Boolean Rings. Duke Math. J. **3**, 455–459 (1937). – [3] McCOY, N. H.: Subrings of Direct Sums. Amer. J. Math. **60**, 374–382 (1938). – [4] ROSENBLOOM, P. C.: Post Algebras I, Postulates and General Theory. Amer. J. Math. **64**, 167–188 (1942). – [5] BIRKHOFF, G.: Subdirect Unions in Universal Algebra. Bull. Amer. Math. Soc. **50**, 764–768 (1944). – [6] WADE, L. I.: Post Algebras and Rings. Duke Math. J. **12**, 389–395 (1945). – [7] FOSTER, A. L.: Generalized "Boolean" Theory of Universal Algebras, Part I: Subdirect Sums and Normal Representation Theorem. Math. Z. **58**, 306–336 (1953), and Part II: Identities and Subdirect Sums of Functionally Complete Algebras. Math. Z. **59**, 191–199 (1953). – [8] FOSTER, A. L.: The Identities of – and Unique Factorization within – Classes of Universal Algebras. Math. Z. **62**, 171–188 (1955). – [9] FOSTER, A. L.: The Generalized Chinese Remainder Theorem for Universal Algebras; Subdirect Factorization. Math. Z. **66**, 452–469 (1957). – [10] FOSTER, A. L.: Ideals and their Structure in Classes of Operational Algebras. Math. Z. **65**, 70–75 (1956).

Dept. of Math., Coll. of Engin., New York University, New York 53, N.Y. (USA)

(Eingegangen am 6. Juli 1959)